

10/507212

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-164885

(P2002-164885A)

(43) 公開日 平成14年6月7日(2002.6.7)

(51) Int.Cl. ⁷	識別記号	F I	テ-リ-ト [*] (参考)
H 0 4 L 9/32		G 0 6 F 13/00	5 4 0 S 5 J 1 0 4
G 0 6 F 13/00	5 4 0	G 0 9 C 1/00	6 4 0 Z
G 0 9 C 1/00	6 4 0		6 6 0 A
	6 6 0		6 6 0 D

G 1 0 K 15/02

審査請求 未請求 請求項の数15 O L (全 37 頁) 最終頁に続く

(21) 出願番号 特願2000-362914(P2000-362914)

(22) 出願日 平成12年11月29日(2000.11.29)

(71) 出願人 000001889

三洋電機株式会社

大阪府守口市京阪本通2丁目5番5号

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番1号

(71) 出願人 000136136

株式会社ピーエフユー

石川県河北郡宇ノ気町宇野気ヌ98番地の2

(74) 代理人 100064746

弁理士 深見 久郎 (外3名)

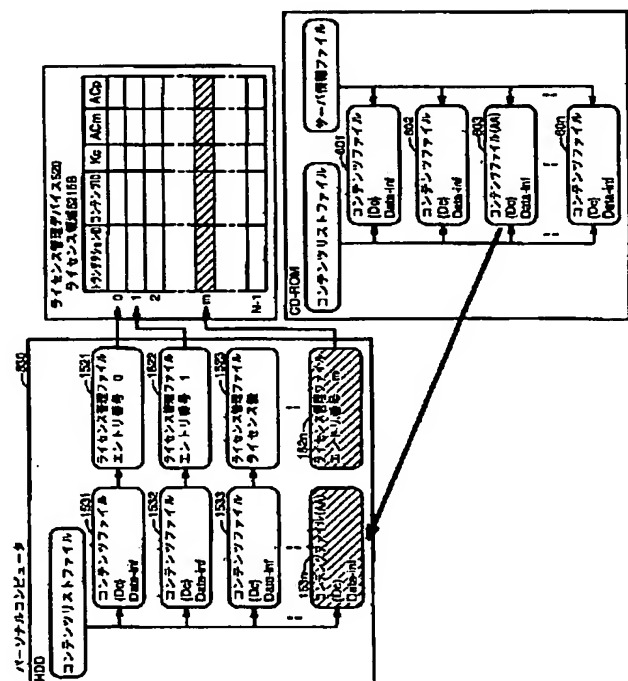
最終頁に続く

(54) 【発明の名称】 データ端末装置

(57) 【要約】

【課題】 記録媒体から暗号化コンテンツデータを取得すると暗号化コンテンツデータを再生するライセンスを取得するデータ端末装置を提供する。

【解決手段】 パーソナルコンピュータは、CD-ROMから暗号化コンテンツデータ、コンテンツファイル601～60n、およびサーバ情報ファイルをハードディスク530にコピーし、サーバ情報ファイルに含まれるアクセス手段およびアクセス先のアドレスに基づいて配信サーバへ暗号化コンテンツデータのライセンスの配信を要求し、ライセンスを受信する。そして、受信したライセンスを内蔵するライセンス管理デバイス520のメモリのライセンス領域5215Bに格納する。



【特許請求の範囲】

【請求項1】 暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを含む記録媒体から前記暗号化コンテンツデータを取得し、前記サーバ情報ファイルに基づいて前記ライセンスを配信サーバから取得するデータ端末装置であって、

前記暗号化コンテンツデータおよび前記サーバ情報ファイルを前記記録媒体から取得する媒体駆動部と、前記媒体駆動部によって取得されたサーバ情報ファイルの内容に応じて前記配信サーバとの接続手段を決定し、その決定した接続手段によって前記配信サーバに接続して前記ライセンスの配信を要求し、前記配信サーバから前記ライセンスを受信する制御部と、前記媒体駆動部によって取得された暗号化コンテンツデータを記憶する記憶部と、前記配信サーバから受信したライセンスを格納するデバイス部とを備えるデータ端末装置。

【請求項2】 前記制御部は、前記媒体駆動部が前記記録媒体から前記サーバ情報ファイルを取得できないとき、ユーザの指示によって前記配信サーバに接続する、請求項1に記載のデータ端末装置。

【請求項3】 前記制御部は、前記決定された接続手段に適したアドレスを前記サーバ情報ファイルから取得し、その取得したアドレスに基づいて前記配信サーバに接続する、請求項1に記載のデータ端末装置。

【請求項4】 前記制御部は、前記デバイス部が保持する認証データを前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証されると前記配信サーバから前記ライセンスを受信する、請求項1から請求項3のいずれか1項に記載のデータ端末装置。

【請求項5】 前記制御部は、前記デバイス部が保持する公開暗号鍵を前記配信サーバへ送信し、前記配信サーバから前記公開暗号鍵によって暗号化されたライセンスを受信する、請求項4に記載のデータ端末装置。

【請求項6】 前記記憶部は、前記媒体駆動部によって前記記録媒体から取得され、かつ、前記暗号化コンテンツデータと、前記暗号化コンテンツデータに関する平文情報とを格納するコンテンツファイルと、前記コンテンツファイルに対応して設けられ、前記デバイス部における前記ライセンスの格納領域を指定するための登録番号を格納するライセンス管理ファイルとをさらに記憶する、請求項1から請求項3のいずれか1項に記載のデータ端末装置。

【請求項7】 前記暗号化コンテンツデータを前記記憶部から取得し、前記取得した暗号化コンテンツデータのライセンスを前記デバイス部から取得し、その取得したライセンスによって前記暗号化コンテンツデータを再生する再生部をさらに備える、請求項1から請求項6のいずれか1項に記載のデータ端末装置。

【請求項8】 前記再生部は、前記デバイス部に対する認証データを保持し、前記認証データが前記デバイス部において認証されると、前記デバイス部から前記ライセンスを取得する、請求項7に記載のデータ端末装置。

【請求項9】 記録媒体から暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを読み取り可能なデータ端末装置から前記暗号化コンテンツデータおよび前記サーバ情報ファイルを取得し、前記サーバ情報ファイルに基づいて前記ライセンスを配信サーバから取得し、前記取得した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録するデータ端末装置であって、前記データ記録装置との間でのデータの授受を制御するインタフェースと、

前記配信サーバとの送受信を行なう送受信部と、前記取得したサーバ情報ファイルの内容に応じて前記配信サーバとの接続手段を決定し、その決定した接続手段によって前記送受信部を介して前記配信サーバに接続して前記ライセンスの配信を要求し、前記配信サーバから前記送受信部を介して前記ライセンスを受信する制御部とを備え、

前記制御部は、前記取得した暗号化コンテンツデータおよびライセンスを前記インタフェースを介して前記データ記録装置へ出力する、データ端末装置。

【請求項10】 前記制御部は、前記データ端末装置から前記サーバ情報ファイルを取得できないとき、ユーザの指示によって前記配信サーバに接続する、請求項9に記載のデータ端末装置。

【請求項11】 前記制御部は、前記決定された接続手段に適したアドレスを前記サーバ情報ファイルから取得し、その取得したアドレスに基づいて前記配信サーバに接続する、請求項9に記載のデータ端末装置。

【請求項12】 前記制御部は、前記データ記録装置が保持する認証データを前記配信サーバへ送信し、前記配信サーバにおいて前記認証データが認証されると前記配信サーバから前記ライセンスを受信する、請求項9から請求項11のいずれか1項に記載のデータ端末装置。

【請求項13】 前記制御部は、前記データ記録装置が保持する公開暗号鍵を前記配信サーバへ送信し、前記配信サーバから前記公開暗号鍵によって暗号化されたライセンスを受信する、請求項12に記載のデータ端末装置。

【請求項14】 前記暗号化コンテンツデータおよび前記ライセンスを前記データ記録装置から取得し、その取得したライセンスによって前記暗号化コンテンツデータを再生する再生部をさらに備える、請求項9から請求項13のいずれか1項に記載のデータ端末装置。

【請求項15】 前記再生部は、前記データ記録装置に対する認証データを保持し、前記認証データが前記デー

タ記録装置において認証されると、前記データ記録装置から前記ライセンスを取得する、請求項14に記載のデータ端末装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【0002】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0003】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【0004】したがって、このような情報通信網上において音楽データや画像データ等の著作権者の権利が存在するコンテンツデータが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0005】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0006】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとりて考えて見ると、通常販売されている音楽データを記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して著作権料として支払うことになっている。

【0007】しかも、CDからMDへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なMDからさらに他のMDに音楽データとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【0008】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信するこ

とは、それ自身が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0009】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されること、あるいは、複製できても利用されることを防止することが必要となる。

【0010】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【0011】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンス鍵と、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【0012】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話に装着する。携帯電話は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【0013】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【0014】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。

【0015】

【発明が解決しようとする課題】しかし、記録媒体に暗号化音楽データを再生するライセンスも記録して販売すると、不正にライセンスが複製されたり、他の装置へ移動されたりするため、通常、記録媒体には暗号化コンテンツデータだけを記録して販売する。そのため、その記録媒体を購入しただけでは、暗号化コンテンツデータを再生することができない。

【0016】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、記録媒体から暗号化コンテンツデータを取得すると暗号化コンテンツデータを再生するライセンスを取得するデータ端末装置を提供することである。

【0017】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを含む記録媒体から暗号化コンテンツデータを取得し、サーバ情報ファイルに基づいてライセンスを配信サーバから取得するデータ端末装置であって、暗号化コンテンツデータおよびサーバ情報ファイルを記録媒体から取得する媒体駆動部と、媒体駆動部によって取得されたサーバ情報ファイルの内容に応じて配信サーバとの接続手段を決定し、その決定した接続手段によって配信サーバに接続してライセンスの配信を要求し、配信サーバからライセンスを受信する制御部と、媒体駆動部によって取得された暗号化コンテンツデータを記憶する記憶部と、配信サーバから受信したライセンスを格納するデバイス部とを備える。

【0018】この発明によるデータ端末装置においては、配信サーバへアクセスするのに必要な情報が記録媒体に記録されたサーバ情報ファイルから取得され、その取得された情報によって暗号化コンテンツデータの再生に必要なライセンスが配信サーバから受信され、データ記録装置に記録される。

【0019】したがって、この発明によれば、記録媒体に記録されたサーバ情報ファイルに基づいて暗号化コンテンツデータを再生するライセンスを取得できる。

【0020】好ましくは、データ端末装置の制御部は、媒体駆動部が記録媒体からサーバ情報ファイルを取得できないとき、ユーザの指示によって配信サーバに接続する。

【0021】記録媒体にサーバ情報ファイルが記録されていないときは、ユーザからの指示を待ち、入力されたユーザの指示に従って配信サーバに接続される。

【0022】したがって、この発明によれば、サーバ情報ファイルを含まない記録媒体から暗号化コンテンツデータを取得した場合でも、配信サーバからライセンスを取得できる。

【0023】好ましくは、データ端末装置の制御部は、決定された接続手段に適したアドレスをサーバ情報ファイルから取得し、その取得したアドレスに基づいて配信サーバに接続する。

【0024】データ端末装置においては、制御部は、サーバ情報ファイルの内容に応じて、たとえば、インターネット、電話回線等の接続手段を決定し、URLまたは電話番号によって配信サーバに接続する。

【0025】したがって、この発明によれば、各種の機

器に応じてライセンスを自動的に取得できる。

【0026】好ましくは、データ端末装置の制御部は、デバイス部が保持する認証データを配信サーバへ送信し、配信サーバにおいて認証データが認証されると配信サーバからライセンスを受信する。

【0027】配信サーバにおいてデータ端末装置が正規の端末装置であると認識されると、データ端末装置は配信サーバからライセンスを受信する。

【0028】したがって、この発明によれば、不正に暗号化コンテンツデータに対してライセンスを配信することを防止できる。

【0029】好ましくは、データ端末装置の制御部は、デバイス部が保持する公開暗号鍵を配信サーバへ送信し、配信サーバから公開暗号鍵によって暗号化されたライセンスを受信する。

【0030】データ端末装置は、公開暗号方式によってライセンスを取得する。したがって、この発明によれば、セキュリティ強度を高くしてライセンスを取得できる。

【0031】好ましくは、データ端末装置の記憶部は、媒体駆動部によって記録媒体から取得され、かつ、暗号化コンテンツデータと、暗号化コンテンツデータに関する平文情報とを格納するコンテンツファイルと、コンテンツファイルに対応して設けられ、デバイス部におけるライセンスの格納領域を指定するための登録番号を格納するライセンス管理ファイルとをさらに記憶する。

【0032】暗号化コンテンツデータの名称に対応して登録番号を格納するライセンス管理ファイルが設けられ、その登録番号によってライセンスを格納する領域が指定される。

【0033】したがって、この発明によれば、登録番号によってライセンスを暗号化コンテンツデータに対応づけることができる。

【0034】好ましくは、データ端末装置は、暗号化コンテンツデータを記憶部から取得し、その取得した暗号化コンテンツデータのライセンスをデバイス部から取得し、その取得したライセンスによって暗号化コンテンツデータを再生する再生部をさらに備える。

【0035】ライセンスが取得されたデータ端末装置においては、再生部によって暗号化コンテンツデータが再生される。

【0036】したがって、この発明によれば、記録媒体から暗号化コンテンツデータを取得し、かつ、暗号化コンテンツデータを再生できる。

【0037】好ましくは、データ端末装置の再生部は、デバイス部に対する認証データを保持し、認証データがデバイス部において認証されると、デバイス部からライセンスを取得する。

【0038】ライセンスを保持するデバイス部において、ライセンスの送信を要求する再生部の正当性が確認

されると再生部はライセンスを取得する。

【0039】したがって、この発明によれば、不正な暗号化コンテンツデータの再生を防止できる。

【0040】また、この発明によるデータ端末装置は、記録媒体から暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスの取得に必要なサーバ情報ファイルとを読み取り可能なデータ端末装置から暗号化コンテンツデータおよびサーバ情報ファイルを取得し、サーバ情報ファイルに基づいてライセンスを配信サーバから取得し、取得した暗号化コンテンツデータおよびライセンスをデータ記録装置に記録するデータ端末装置であって、データ記録装置との間でのデータの授受を制御するインタフェースと、配信サーバとの送受信を行なう送受信部と、取得したサーバ情報ファイルの内容に応じて配信サーバとの接続手段を決定し、その決定した接続手段によって送受信部を介して配信サーバに接続してライセンスの配信を要求し、配信サーバから送受信部を介してライセンスを受信する制御部とを備え、制御部は、取得した暗号化コンテンツデータおよびライセンスをインタフェースを介してデータ記録装置へ出力する。

【0041】記録媒体の駆動手段を持たないデータ端末装置では、記録媒体の駆動手段を持つデータ端末装置から暗号化コンテンツデータおよびサーバ情報ファイルを送ってもらい、そのサーバ情報ファイルに基づいて暗号化コンテンツデータを再生するライセンスを配信サーバから受信する。

【0042】したがって、この発明によれば、記録媒体の駆動手段を持たないデータ端末装置のユーザでも、記録媒体に記録されて販売された暗号化コンテンツデータを再生可能である。

【0043】好ましくは、データ端末装置の制御部は、データ端末装置からサーバ情報ファイルを取得できないとき、ユーザの指示によって配信サーバに接続する。

【0044】データ端末装置からサーバ情報ファイルが送られてこないときは、ユーザからの指示を待ち、入力されたユーザの指示に従って配信サーバに接続される。

【0045】したがって、この発明によれば、サーバ情報ファイルを含まない記録媒体から暗号化コンテンツデータを取得した場合でも、配信サーバからライセンスを取得できる。

【0046】好ましくは、データ端末装置の制御部は、決定された接続手段に適したアドレスをサーバ情報ファイルから取得し、その取得したアドレスに基づいて配信サーバに接続する。

【0047】データ端末装置においては、制御部は、サーバ情報ファイルの内容に応じて、たとえば、インターネット、電話回線等の接続手段を決定し、URLまたは電話番号によって配信サーバに接続する。

【0048】したがって、この発明によれば、各種の機

器に応じてライセンスを自動的に取得できる。

【0049】好ましくは、データ端末装置の制御部は、データ記録装置が保持する認証データを配信サーバへ送信し、配信サーバにおいて認証データが認証されると配信サーバからライセンスを受信する。

【0050】配信サーバにおいてデータ端末装置が正規の端末装置であると認識されると、データ端末装置は配信サーバからライセンスを受信する。

【0051】したがって、この発明によれば、不正に暗号化コンテンツデータに対してライセンスを配信することを防止できる。

【0052】好ましくは、データ端末装置の制御部は、データ記録装置が保持する公開暗号鍵を配信サーバへ送信し、配信サーバから公開暗号鍵によって暗号化されたライセンスを受信する。

【0053】データ端末装置は、公開暗号方式によってライセンスを取得する。したがって、この発明によれば、セキュリティ強度を高くしてライセンスを取得できる。

【0054】好ましくは、データ端末装置は、暗号化コンテンツデータおよびライセンスをデータ記録装置から取得し、その取得したライセンスによって暗号化コンテンツデータを再生する再生部をさらに備える。

【0055】ライセンスが取得されたデータ端末装置においては、再生部によって暗号化コンテンツデータが再生される。

【0056】したがって、この発明によれば、記録媒体の駆動手段を持たないデータ端末装置においても、記録媒体から暗号化コンテンツデータを取得し、かつ、暗号化コンテンツデータを再生できる。

【0057】好ましくは、データ端末装置の再生部は、データ記録装置に対する認証データを保持し、認証データがデータ記録装置において認証されると、データ記録装置からライセンスを取得する。

【0058】ライセンスを保持するデータ記録装置において、ライセンスの送信を要求する再生部の正当性が確認されると再生部はライセンスを取得する。

【0059】したがって、この発明によれば、不正な暗号化コンテンツデータの再生を防止できる。

【0060】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【0061】図1は、本発明によるデータ端末装置（パーソナルコンピュータまたは携帯電話機）がCD-ROMから暗号化コンテンツデータを取得し、その取得した暗号化コンテンツデータのライセンスを配信サーバから受信するデータ配信システムの全体構成を概念的に説明するための概略図である。

【0062】なお、以下ではインターネットを介して音

楽データを各パーソナルコンピュータのユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画データ等を配信する場合においても適用することが可能なものである。

【0063】図1を参照して、パーソナルコンピュータ50は、CD-ROM60から暗号化音楽データを取得すると、モデム40およびインターネット網30を介して、暗号化コンテンツデータを再生するライセンスの配信要求（配信リクエスト）を配信サーバ10に送信する。著作権の存在する音楽データを管理する配信サーバ10は、データ配信を求めてアクセスして来たパーソナルコンピュータのユーザが所有するパーソナルコンピュータ50が正当な認証データを持つか否か、すなわち、正規のパーソナルコンピュータであるか否かの認証処理を行ない、正当なパーソナルコンピュータに対して所定の暗号方式によりライセンスを暗号化した上で、このような暗号化したライセンスをパーソナルコンピュータ50に配信する。

【0064】また、パーソナルコンピュータ50は、CD-ROM60から暗号化コンテンツデータを取込み、その取込んだ暗号化コンテンツデータをUSB（Universal Serial Bus）ケーブル70を介して携帯電話機100へ送信する。そして、携帯電話機100は、装着されたメモリカード110に暗号化コンテンツデータを記録し、その暗号化コンテンツデータを再生するためのライセンスを、携帯電話網を介して配信サーバ10へライセンスの配信要求を送信する。そうすると、配信サーバ10は、メモリカードの正当性を認証データによって確認し、正規のメモリカードからのアクセスであることが判明すれば、携帯電話網を介してライセンスをメモリカード110に配信するために、所定の暗号化を施した暗号化ライセンスを通信キャリア20に渡す。これによって、パーソナルコンピュータ50から取得した暗号化コンテンツデータを再生するためのライセンスがメモリカード110に送信される。携帯電話機100は、メモリカード110に記録された暗号化コンテンツデータをライセンスによって再生するコンテンツ再生デバイス（図示せず）を内蔵しており、携帯電話機100のユーザは、携帯電話機100に接続されたヘッドホン130を介してコンテンツ再生デバイスによって再生された音楽を聞くことができる。

【0065】通常、携帯電話機は、CD-ROMから、直接、暗号化コンテンツデータを取得することができないため、パーソナルコンピュータ50を介してCD-ROMから暗号化コンテンツデータを取得できる。

【0066】したがって、図1に示すデータ配信システムにおいては、パーソナルコンピュータ50は、モデム

40およびインターネット網30を介して配信サーバ10からライセンスを受信するとともに、CD-ROM60から暗号化コンテンツデータを取得する。また、携帯電話機100に装着されたメモリカード110は、パーソナルコンピュータ50がCD-ROM60から取得した暗号化コンテンツデータを受信し、その暗号化コンテンツデータを再生するライセンスを配信サーバ10から受信する。携帯電話機100のユーザは、パーソナルコンピュータ50を介することによってCD-ROMから暗号化コンテンツデータを取得することが可能となる。

【0067】このような構成とすることで、正規なパーソナルコンピュータまたはメモリカードでないと、配信サーバ10から暗号化コンテンツデータのライセンスを受信することが困難な構成となる。

【0068】しかも、配信サーバ10において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、パーソナルコンピュータのユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、インターネット網の使用料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0069】図1に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0070】本発明の実施の形態においては、特に、配信、移動、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を携帯電話機またはパーソナルコンピュータとも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0071】なお、以下の説明においては、配信サーバ10から、各パーソナルコンピュータ等に暗号化コンテンツデータのライセンスを伝送する処理を「配信」と称することとする。

【0072】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0073】まず、Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツ

データ {Dc} Kcがこの形式でCD-ROM60よりパーソナルコンピュータ50に取込まれる。

【0074】なお、以下においては、{Y} Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0075】また、CD-ROM60からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc-infがパーソナルコンピュータ50に取込まれる。

【0076】さらに、配信サーバ10からは、暗号化コンテンツデータのライセンスがパーソナルコンピュータ50またはメモリカード110に配信される。また、配信サーバ10からのライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ10とパーソナルコンピュータ50との間、または配信サーバ10と携帯電話機100との間でやり取りされる。

【0077】またさらに、ライセンスとしては、ライセンス鍵Kc、コンテンツデータDcを識別するためのコードであるコンテンツIDや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制限情報ACmおよびデータ再生端末における再生に関する制御情報である再生制限情報ACpが存在する。具体的には、アクセス制御情報ACmはメモリカード、ライセンス管理モジュールおよびライセンス管理モジュールからのライセンス又はライセンス鍵を外部に出力に対するに当たっての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ACpは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【0078】以後、トランザクションIDとコンテンツIDとを併せてライセンスIDと総称し、ライセンス鍵KcとライセンスIDとアクセス制限情報ACmと再生制限情報ACpとを併せて、ライセンスと総称することとする。

【0079】本発明の実施の形態においては、記録装置（メモリカード、またはライセンス管理デバイス）やコンテンツデータを再生する携帯電話機のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストCRL（Certificate Revocation List）の運用を行なう。以下では、必要に応じて記号CRLによって禁

止クラスリスト内のデータを表わすこともある。

【0080】禁止クラスリスト関連情報には、ライセンスの配信、移動、チェックアウト、チェックイン、および再生が禁止される携帯電話機、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスのクラスをリストアップした禁止クラスリストデータCRLが含まれる。

【0081】禁止クラスリストデータCRLは、配信サーバ10内で管理されるとともに、メモリカード110や、パーソナルコンピュータ50内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび/またはライセンス鍵等のライセンスを配信する際に、パーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）から受取った禁止クラスリストの更新日時を、所有する禁止クラスリストCRLの更新日時と比較して更新されていないと判断されたとき、更新された禁止クラスリストをパーソナルコンピュータに配信する。また、ライセンス管理モジュール、ライセンス管理デバイス、および携帯電話機100の間でも禁止クラスリストはやり取りされ、そのデータ変更も上述したのと同じである。さらに、禁止クラスリストの変更については、変更点のみを反映した差分データである差分CRLを配信サーバ10側より発生して、これに応じてメモリカード、ハードディスク、およびライセンス管理デバイス内の禁止クラスリストCRLに追加する構成とするも可能である。

【0082】このように、禁止クラスリストCRLを、配信サーバのみならずメモリカードまたはパーソナルコンピュータ内においても保持運用することによって、クラス固有すなわち、携帯電話機およびメモリカードまたはパーソナルコンピュータの種類に固有の復号鍵が破られた、携帯電話機およびメモリカードまたはパーソナルコンピュータへのライセンス鍵の供給を禁止する。このため、携帯電話機またはパーソナルコンピュータではコンテンツデータの再生が、メモリカードでは新たなライセンスの取得が行なえなくなる。

【0083】このように、メモリカードまたはライセンス管理デバイス内の禁止クラスリストCRLは配信時に逐次データを更新する構成とする。また、メモリカードにおける禁止クラスリストCRLの管理は、上位レベルとは独立にメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって制御されるハードディスクでタンパーレジスタントモジュール（Tamper Resistance Module）に記録する等によって、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータCRLを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なもの

とすることができる。

【0084】図3は、図1に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【0085】携帯電話機、メモリカード、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス、およびライセンス管理モジュールには固有の公開暗号鍵K P p yおよびK P m wがそれぞれ設けられ、公開暗号鍵K P p yおよびK P m wは携帯電話機に固有の秘密復号鍵K p yおよびメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の秘密復号鍵K m wによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、携帯電話機、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称する。

【0086】また、コンテンツ再生デバイス（携帯電話機）のクラス証明書としてC p yが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてC m wが設けられる。

【0087】これらのクラス証明書は、コンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる情報を有する。クラス鍵による暗号が破られた、すなわち、秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンス発行の禁止対象となる。

【0088】これらのコンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の公開暗号鍵およびクラス証明書は、認証データ {K P p y / C p y} K P a の形式または認証データ {K P m w / C m w} K P a の形式で、出荷時にデータ再生デバイス（携帯電話機）、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールにそれぞれ記録される。後ほど詳細に説明するが、K P a は配信システム全体で共通の公開認証鍵である。

【0089】メモリカード外とメモリカード間でのデータ授受、またはライセンス管理デバイス外とライセンス管理デバイス間でのデータ授受、またはライセンス管理モジュール外とライセンス管理モジュール間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ10、携帯電話機100、メモリカード110、ライセンス管理デバイス、ライセンス管理モジュールにおいて生成される共通鍵K s 1～K s 3が用いられる。

【0090】ここで、共通鍵K s 1～K s 3は、配信サーバ、携帯電話機もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」

」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵K s 1～K s 3を「セッションキー」とも呼ぶこととする。

【0091】これらのセッションキーK s 1～K s 3は、各通信セッションごとに固有の値を有することにより、配信サーバ、携帯電話機、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって管理される。具体的には、セッションキーK s 1は、配信サーバによって配信セッションごとに発生される。セッションキーK s 2は、メモリカード、ライセンス管理デバイス、ライセンス管理モジュールによって配信セッションおよび再生セッションごとに発生し、セッションキーK s 3は、携帯電話機において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【0092】また、メモリカード110、ライセンス管理デバイス、およびライセンス管理モジュール内のデータ処理を管理するための鍵として、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールという媒体ごとに設定される公開暗号鍵K P m c xと、公開暗号鍵K P m c xで暗号化されたデータを復号することが可能なメモリカードごとに固有の秘密復号鍵K m c xが存在する。

【0093】図4は、図1に示した配信サーバ10の構成を示す概略ブロック図である。配信サーバ10は、暗号化コンテンツデータのコンテンツID等の配信情報を保持するための情報データベース304と、パーソナルコンピュータの各ユーザごとにライセンス鍵等へのアクセス開始に従った課金情報を保持するための課金データベース302と、禁止クラスリストC R Lを管理するC R Lデータベース306と、情報データベース304に保持されたライセンスによって再生されるコンテンツデータのメニューを保持するメニューデータベース307と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションID等の配信に関するログを保持する配信記録データベース308と、情報データベース304、課金データベース302、C R Lデータベース306、メニューデータベース307、および配信記録データベース308からのデータをバスB S 1を介して受取り、所定の処理を行なうためのデータ処理部310と、通信網を介して、配信キャリア20とデータ処理部310との間でデータ授受を行なうための通信装置350とを備える。

【0094】データ処理部310は、バスB S 1上のデータに応じて、データ処理部310の動作を制御するための配信制御部315と、配信制御部315に制御され

て、配信セッション時にセッションキーKs1を発生するためのセッションキー発生部316と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ{K P m w / / C m w} K P aを復号するための公開認証鍵を保持する認証鍵保持部313と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ{K P m w / / C m w} K P aを通信装置350およびバスBS1を介して受けて、認証鍵保持部313からの公開認証鍵K P aによって復号処理を行なう復号処理部312と、セッションキー発生部316より生成されたセッションキーKs1を復号処理部312によって得られた公開暗号鍵K P m wを用いて暗号化して、バスBS1に出力するための暗号処理部318と、セッションキーKs1によって暗号化された上で送信されたデータをバスBS1より受けて、復号処理を行なう復号処理部320を含む。

【0095】データ処理部310は、さらに、配信制御部315から与えられるライセンス鍵Kcおよび再生制限情報A C mを、復号処理部320によって得られたメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の公開暗号鍵K P m c xによって暗号化するための暗号処理部326と、暗号処理部326の出力を、復号処理部320から与えられるセッションキーKs2によってさらに暗号化してバスBS1に出力するための暗号処理部328を含む。

【0096】配信サーバ10の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0097】図5は、図1に示したパーソナルコンピュータ50の構成を説明するための概略ブロック図である。パーソナルコンピュータ50は、パーソナルコンピュータ50の各部のデータ授受を行なうためのバスBS2と、インターネット網を介してライセンス管理デバイス520またはライセンス管理モジュール511に暗号化コンテンツデータのライセンスを配信サーバ10から受信するために、配信サーバ10との間でデータの授受を制御するとともに、CD-ROMドライブ540を介してCD-ROMから暗号化コンテンツデータを取得する際の制御を行なうためのコントローラ510と、配信サーバ10からのライセンスの受信を行なう際に配信サーバ10との間で各種の鍵のやり取りを行ない、CD-ROM60から取得された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス520と、コントローラ510に含まれ、CD-ROM60からの暗号化コンテンツデータの取得をプログラムによって実行するコンテンツ管理モジュール511を含む。

【0098】ライセンス管理デバイス520は、暗号化コンテンツデータのライセンスを配信サーバ10から受

信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理するものであるため、高いセキュリティレベルでライセンスの受信とライセンスの管理とを行なうことができるものである。

【0099】パーソナルコンピュータ50は、さらに、CD-ROMドライブ540を介してCD-ROM60から取得した暗号化コンテンツデータおよびコンテンツファイルと、ライセンス管理デバイス520によって受信した暗号化コンテンツデータのライセンスの格納する領域を指定するためのエントリ番号を暗号化コンテンツデータのファイル名と対応付けて格納するライセンス管理ファイルとを記憶するハードディスク(HDD)530を含む。なお、コンテンツリストファイルの詳細については後述する。

【0100】パーソナルコンピュータ50は、さらに、暗号化コンテンツデータを携帯電話機100等に通信する際にコントローラ510と端子580との間でデータの授受を制御するためのUSBインタフェース550と、CD-ROM60からコンテンツデータを取得するためのCD-ROMドライブ540と、ユーザからの指示を入力するためのキーボード560と、各種の情報を視覚的にユーザに与えるためのディスプレイ570と、USBケーブル70を接続するための端子580と、暗号化コンテンツデータをライセンスによって再生するためのコンテンツ再生デバイス1550を含む。

【0101】このように、パーソナルコンピュータ50は、配信サーバ10からインターネット網30を介してライセンスを受信するためのライセンス管理デバイス520と、CD-ROM60から暗号化コンテンツデータを取得するためのCD-ROMドライブ540とを内蔵するものである。

【0102】図6は、図1に示した携帯電話機100の構成を説明するための概略ブロック図である。

【0103】携帯電話機100は、携帯電話機100の各部のデータ授受を行なうためのバスBS3と、携帯電話網により無線伝送される信号を受信するためのアンテナ102と、アンテナ102からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部104と、バスBS3を介して携帯電話機100の動作を制御するためのコントローラ1106と、外部からの指示を携帯電話機100に与えるための操作パネル1108と、コントローラ1106等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル1110を含む。

【0104】携帯電話機100は、さらに、配信サーバ10からのコンテンツデータ(音楽データ)を記憶しかつ復号化処理するための着脱可能なメモリカード1110と、メモリカード1110とバスBS3との間のデータの授受を制御するためのメモリインタフェース1200

と、パーソナルコンピュータ50から暗号化コンテンツデータおよびライセンスを受信する際にバスBS3と端子1114との間のデータ授受を制御するためのUSBインタフェース1112と、USBケーブル70を接続するための端子1114とを含む。

【0105】携帯電話機100は、さらに、携帯電話機の種類(クラス)ごとにそれぞれ設定される、公開暗号鍵K_{Pp1}およびクラス証明書C_{p1}を公開復号鍵K_{Pa}で復号することでその正当性を認証できる状態に暗号化した認証データ{K_{Pp1}/C_{p1}}K_{Pa}を保持する認証データ保持部1500を含む。ここで、携帯電話機(データ端末装置)100のクラスyは、y=1であるとする。

【0106】携帯電話機100は、さらに、携帯電話機(コンテンツ再生デバイス)固有の復号鍵であるK_{p1}を保持するK_{p1}保持部1502と、バスBS3から受けたデータをK_{p1}によって復号しメモリカード110によって発生されたセッションキーK_{s2}を得る復号処理部1504とを含む。

【0107】携帯電話機100は、さらに、メモリカード110に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード110との間でバスBS3上においてやり取りされるデータを暗号化するためのセッションキーK_{s3}を乱数等により発生するセッションキー発生部1508と、暗号化コンテンツデータの再生セッションにおいてメモリカード110からライセンス鍵K_cおよび再生制限情報A_{Cp}を受取る際に、セッションキー発生部1508により発生されたセッションキーK_{s3}を復号処理部1504によって得られたセッションキーK_{s2}によって暗号化しバスBS3に出力する暗号処理部1506とを含む。

【0108】携帯電話機100は、さらに、バスBS3上のデータをセッションキーK_{s3}によって復号して、コンテンツ鍵K_cおよび再生制限情報A_{Cp}を出力する復号処理部1510と、バスBS3より暗号化コンテンツデータ{D_c}K_cを受けて、復号処理部1510より取得したライセンス鍵K_cによって復号しコンテンツデータを出力する復号処理部1516と、復号処理部1516の出力を受けてコンテンツデータを再生するための音楽再生部1518と、音楽再生部1518の出力をデジタル信号からアナログ信号に変換するDA変換器1519と、DA変換器1519の出力をヘッドホンなどの外部出力装置(図示省略)へ出力するための端子1530とを含む。

【0109】なお、図7においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス1550を構成する。また、図7においては、説明の簡素化のため、携帯電話機のうち本発明の音楽データの再生にかかわるブロックのみを記載し、携帯電話機が本来備えている通話機能に関

するブロックについては、一部記載を省略している。

【0110】携帯電話機100の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【0111】図7は、メモリカード110の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、K_{Pmw}およびK_{m_w}が設けられ、メモリカードのクラス証明書C_{mw}が設けられるが、メモリカード110においては、これらは自然数w=3でそれぞれ表わされるものとする。

【0112】したがって、メモリカード110は、認証データ{K_{Pm3}/C_{m3}}K_{Pa}を保持する認証データ保持部1400と、メモリカードごとに設定される固有の復号鍵であるK_{mc4}を保持するK_{mc}保持部1402と、メモリカードの種類ごとに設定される固有の秘密復号鍵K_{m3}を保持するK_m保持部1421と、K_{mc4}によって復号可能な公開暗号鍵K_{Pmc4}を保持するK_{Pmc}保持部1416とを含む。認証データ保持部1400は、メモリカードの種類およびクラスごとにそれぞれ設定される秘密暗号鍵K_{Pm3}およびクラス証明書C_{m3}を公開認証鍵K_{Pa}で復号することでその正当性を認証できる状態に暗号化した認証データ{K_{Pm3}/C_{m3}}K_{Pa}として保持する。

【0113】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【0114】メモリカード110は、さらに、メモリインタフェース1200との間で信号を端子1426を介して授受するインタフェース1424と、インタフェース1424との間で信号をやり取りするバスBS4と、バスBS4にインタフェース1424から与えられるデータから、メモリカードの種類ごとに固有の秘密復号鍵K_{m3}をK_m保持部1421から受けて、配信サーバ10が配信セッションにおいて生成したセッションキーK_{s1}を接点Paに出力する復号処理部1422と、K_{Pa}保持部1414から認証鍵K_{Pa}を受けて、バスBS4に与えられるデータからK_{Pa}による復号処理を実行して復号結果を暗号処理部1410に出力する復号処理部1408と、切換スイッチ1442によって選択的に与えられる鍵によって、切換スイッチ1446によって選択的に与えられるデータを暗号化してバスBS4に出力する暗号処理部1406とを含む。

【0115】メモリカード110は、さらに、再生セッションにおいてセッションキーK_{s2}を発生するセッションキー発生部1418と、セッションキー発生部1418の出力したセッションキーK_{s2}を復号処理部1408によって得られる公開暗号鍵K_{Ppy}もしくはK_P

mwによって暗号化してバスBS4に送出する暗号処理部1410と、バスBS4よりセッションキーKs2によって暗号化されたデータを受けてセッションキー発生部1418より得たセッションキーKs2によって復号する復号処理部1412と、暗号化コンテンツデータの再生セッションにおいてメモリ1415から読出されたライセンス鍵Kcおよび再生期限ACpを、復号処理部1412で復号されたメモリカード110に固有の公開暗号鍵KPmcxで暗号化する暗号処理部1417とを含む。

【0116】メモリカード110は、さらに、バスBS4上のデータを公開暗号鍵KPmc4と対をなすメモリカード110固有の秘密復号鍵Kmc4によって復号するための復号処理部1404と、禁止クラスリストデータCRLと、暗号化コンテンツデータ{Dc}Kcと、暗号化コンテンツデータ{Dc}Kcを再生するためのライセンス(Kc, ACp, ACm, ライセンスID)と、付加情報Data-infと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスBS4より受けて格納するためのメモリ1415とを含む。メモリ1415は、例えば半導体メモリによって構成される。また、メモリ1515は、禁止クラスリストCRLを記録したCRL領域1415Aと、ライセンスを記録したライセンス領域1415Bと、暗号化コンテンツデータ{Dc}Kc、暗号化コンテンツデータの関連情報Dc-inf、再生リスト、およびライセンス管理ファイルを記録したデータ領域1415Cとから成る。

【0117】ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【0118】また、ライセンス領域1415Bは、ライセンス(コンテンツ鍵Kc、再生制御情報ACp、アクセス制限情報ACm、ライセンスID)を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【0119】メモリカード110は、さらに、バスBS4を介して外部との間でデータ授受を行ない、バスBS4との間で再生情報等を受けて、メモリカード110の動作を制御するためのコントローラ1420とを含む。

【0120】なお、データ領域1415Cを除く全ての構成は、耐タンパモジュール領域に構成される。

【0121】以降では、簡単化のためアクセス制御情報ACmは再生回数の制限を行なう制御情報である再生回数のみを、再生回路制御情報ACpは再生可能な期限を規定する制御情報である再生期限のみを制限するものとし、アクセス制御情報ACmおよび再生回路制御情報ACpを、それぞれ、再生回数制限ACm、再生期限AC

pと称するものとする。

【0122】図8は、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス520の構成を示す概略ブロック図である。ライセンス管理デバイス520は、基本的にメモリカード110と同じ構成から成る。ライセンス管理デバイス520の認証データ保持部5200、Kmc保持部5202、復号処理部5204、暗号処理部5206、復号処理部5208、暗号処理部5210、復号処理部5212、KPa保持部5214、KPmc保持部5216、暗号処理部5217、セッションキー発生部5218、コントローラ5220、Km保持部5221、復号処理部5222、インタフェース5224、端子5226、切換スイッチ5242、5246は、それぞれ、メモリカード110の認証データ保持部1400、Kmc保持部1402、復号処理部1404、暗号処理部1406、復号処理部1408、暗号処理部1410、復号処理部1412、KPa保持部1414、KPmc保持部1416、暗号処理部1417、セッションキー発生部1418、コントローラ1420、Km保持部1421、復号処理部1422、インタフェース1424、端子1426、切換スイッチ1442、1446と同じである。ただし、認証データ保持部5200は、{KPm7//Cm7}KPaの形式で認証データを保持し、Km保持部5202は、秘密復号鍵Km7を保持し、Kmc保持部5221は、秘密復号鍵Kmc8を保持する。

【0123】ライセンス管理デバイス520は、禁止クラスリストCRLとライセンス(Kc, ACp, ACm, ライセンスID)とを記録するメモリ5215を、メモリカード110のメモリ1415に代えて含む。メモリ5215は、禁止クラスリストCRLを記録したCRL領域5215Aと、ライセンスを記録したライセンス領域5215Bとから成る。

【0124】以下、図1に示すデータ配信システムにおける各セッションの動作について説明する。

【0125】【配信】次に、図1に示すデータ配信システムにおいて、配信サーバ10からパーソナルコンピュータ50のライセンス管理デバイス520へ暗号化コンテンツデータのライセンスを配信する動作について説明する。

【0126】図9～図13は、図1に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ50に内蔵されたライセンス管理デバイス520への配信動作(以下、配信セッションともいう)を説明するための第1～第5のフローチャートである。

【0127】図9を参照して、パーソナルコンピュータ50のユーザからキーボード560を介してCD-ROM60から暗号化コンテンツデータを取得する指示が入力されると、パーソナルコンピュータ50のコントロー

ラ510は、CD-ROMに記録されたコンテンツリストに従って、コンテンツデータのリストを作成し、ライセンスの購入要求の確認を行なう(ステップS78)。そして、コンテンツIDの指定による配信リクエストがなされ(ステップS80)、キーボード560を介して暗号化コンテンツデータのライセンスを購入するための購入条件ACが入力される(ステップS82)。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Kcを購入するために、暗号化コンテンツデータの再生回数制限ACm、および再生期限ACpを設定して購入条件ACが入力される。

【0128】暗号化コンテンツデータの購入条件ACが入力されると、CD-ROMからサーバ情報ファイルが取得されたか否かが判別され(ステップS84)、サーバ情報ファイルが取得されなかったときはステップS100へ移行し、サーバ情報ファイルが取得されたときは、次のステップS86へ移行する(ステップS84)。

【0129】ステップS84において、サーバ情報ファイルが取得されたと判別されると、配信リクエストされたコンテンツに対する情報の有無が判別される(ステップS86)。つまり、「このコンテンツデータを取得するためには、インターネットを用いなさい。」とか、「このコンテンツデータを取得するためには、電話回線を用いなさい。」とかのようにCD-ROM60から取得された暗号化コンテンツデータの種類に応じて配信サーバ10に接続するための接続手段に関する情報や、「このコンテンツに対しては、どこのサーバへアクセスしなさい」とかのライセンスを取得するためにアクセスすべきアドレス等の情報の有無を判別する。そして、ステップS86において、このような情報がないときは、ステップS100へ移行し、情報があるときは、ステップS88へ移行する。

【0130】ステップS86において、コンテンツデータに対する情報が有ると判別されると、配信サーバ10との接続方法の確認が成される(ステップS88)。つまり、インターネットによって接続するのか、電話回線によって接続するのか、それとも、インターネットおよび電話回線で接続しないのかの確認が行われる。そして、電話回線で接続するときは、ステップS90へ移行し、インターネットによって接続するときはステップS94へ移行し、インターネットおよび電話回線で接続できないときはステップS190へ移行して配信セッションは終了する。

【0131】ステップS88において電話回線によって接続することが確認されると、サーバ情報ファイルから電話番号が取得され(ステップS90)、取得した電話番号をダイヤルしてモデム経由で配信サーバ10に接続する(ステップS92)。一方、ステップS88において、インターネットによって接続することが確認される

と、回線が接続されたか否かの確認が行われ(ステップS94)、未接続のときはステップS190へ移行して配信セッションは終了し、回線の接続が確認されたときはステップS96へ移行する(ステップS94)。

【0132】ステップS94において、回線に接続が確認されると、サーバ情報ファイルからURLが取得され(ステップS96)、URLに基づいて配信サーバ10と接続される(ステップS98)。また、ステップS84にサーバ情報ファイルが無いと判別されたとき、またはステップS86においてコンテンツデータに対する情報が無いと判別されたとき、ユーザによって配信サーバ10との接続が指示され(ステップS100)、配信サーバ10との接続が確認される(ステップS102)。ステップS102において、未接続と判別されるとステップS190へ移行して配信セッションは終了し、接続と判別されると、次のステップS104へ移行する。

【0133】図10を参照して、ステップS92またはステップS98またはステップS102の後、コントローラ510は、バスBS2を介してライセンス管理デバイス520へ認証データの出力指示を与える(ステップS104)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して認証データの出力指示を受取る。そして、コントローラ5220は、バスBS5を介して認証データ保持部5200から認証データ{K P m 7 / / C m 7} K P aを読み出し、{K P m 7 / / C m 7} K P aをバスBS5、インタフェース5224および端子5226を介して出力する(ステップS106)。

【0134】パーソナルコンピュータ50のコントローラ510は、ライセンス管理デバイス520からの認証データ{K P m 7 / / C m 7} K P aに加えて、コンテンツID、ライセンス購入条件のデータAC、および配信リクエストを配信サーバ10に対して送信する(ステップS108)。

【0135】配信サーバ10では、パーソナルコンピュータ50から配信リクエスト、コンテンツID、認証データ{K P m 7 / / C m 7} K P a、およびライセンス購入条件のデータACを受信し(ステップS110)、復号処理部312においてライセンス管理デバイス520から出力された認証データを公開認証鍵K P aで復号処理を実行する(ステップS112)。

【0136】配信制御部315は、復号処理部312における復号処理結果から、処理が正常に行なわれたか否か、すなわち、ライセンス管理デバイス520が正規のライセンス管デバイスからの公開暗号鍵K P m 7と証明書C m 7とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS114)。正当な認証データであると判断された

場合、配信制御部315は、公開暗号鍵K P m 7および証明書C m 7を承認し、受理する。そして、次の処理（ステップS 116）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵K P m 7および証明書C m 7を受理しないで処理を終了する（ステップS 198）。

【0137】認証の結果、正規の機器であることが認識されると、配信制御部315は、次に、ライセンス管理デバイスのクラス証明書C m 7が禁止クラスリストC R LにリストアップされているかどうかをC R Lデータベース306に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップS 198）。

【0138】一方、ライセンス管理デバイス520のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップS 116）。

【0139】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ10において、配信制御部315は、配信を特定するための管理コードであるトランザクションIDを生成する（ステップS 118）。また、セッションキー発生部316は、配信のためのセッションキーK s 1を生成する（ステップS 120）。セッションキーK s 1は、復号処理部312によって得られたライセンス管理デバイス520に対応する公開暗号鍵K P m 7によって、暗号処理部318によって暗号化される（ステップS 122）。

【0140】トランザクションIDおよび暗号化されたセッションキーK s 1は、トランザクションID／／{K s 1} K m 7として、バスBS 1および通信装置350を介して外部に出力される（ステップS 124）。

【0141】図11を参照して、パーソナルコンピュータ50が、トランザクションID／／{K s 1} K m 7を受信すると（ステップS 126）、コントローラ510は、トランザクションID／／{K s 1} K m 7をライセンス管理デバイス520に入力する（ステップS 128）。そうすると、ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS 5に与えられた受信データを、復号処理部5222が、保持部5221に保持されるライセンス管理デバイス520に固有の秘密復号鍵K m 7により復号処理することにより、セッションキーK s 1を復号し、セッションキーK s 1を受理する（ステップS 130）。

【0142】コントローラ5220は、配信サーバ10で生成されたセッションキーK s 1の受理を確認すると、セッションキー発生部5218に対してライセンス管理デバイス520において配信動作時に生成されるセッションキーK s 2の生成を指示する。そして、セッ

ションキー発生部5218は、セッションキーK s 2を生成する（ステップS 132）。

【0143】また、配信セッションにおいては、コントローラ5220は、ライセンス管理デバイス520内のメモリ5215に記録されている禁止クラスリストの更新日時C R L d a t eをメモリ1415から抽出して切換スイッチ5246に出力する（ステップS 134）。

【0144】暗号処理部5206は、切換スイッチ5242の接点P aを介して復号処理部5222より与えられるセッションキーK s 1によって、切換スイッチ5246の接点を順次切換えることによって与えられるセッションキーK s 2、公開暗号鍵K P m c 8および更新日時C R L d a t eを1つのデータ列として暗号化して、{K s 2／／K P m c 8／／C R L d a t e} K s 1をバスBS 3に出力する（ステップS 136）。

【0145】バスBS 3に出力された暗号化データ{K s 2／／K P m c 8／／C R L d a t e} K s 1は、バスBS 3からインタフェース5224および端子5226を介してパーソナルコンピュータ50に出力され、パーソナルコンピュータ50から配信サーバ10に送信される（ステップS 138）。

【0146】配信サーバ10は、トランザクションID／／{K s 2／／K P m c 8／／C R L d a t e} K s 1を受信して、復号処理部320においてセッションキーK s 1による復号処理を実行し、ライセンス管理デバイス520で生成されたセッションキーK s 2、ライセンス管理デバイス520固有の公開暗号鍵K P m c 8およびライセンス管理デバイス520における禁止クラスリストの更新日時C R L d a t eを受理する（ステップS 142）。

【0147】配信制御部315は、ステップS 110で取得したコンテンツIDおよびライセンス購入条件のデータA Cに従って、アクセス制限情報A C mおよび再生期限A C pを生成する（ステップS 144）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵K cを情報データベース304より取得する（ステップS 146）。

【0148】配信制御部315は、生成したライセンス、すなわち、トランザクションID、コンテンツID、ライセンス鍵K c、再生期限A C p、およびアクセス制限情報A C mを暗号処理部326に与える。暗号処理部326は、復号処理部320によって得られたライセンス管理デバイス520固有の公開暗号鍵K P m c 8によってライセンスを暗号化して暗号化データ{トランザクションID／／コンテンツID／／K c／／A C m／／A C p} K m c 8を生成する（ステップS 148）。

【0149】図12を参照して、配信サーバ10において、ライセンス管理デバイス520から送信された禁止クラスリスト更新日時C R L d a t eから、ライセンス

管理デバイス520が保持する禁止クラスリストCRLが最新か否かが判断され、最新と判断されたとき、ステップS152へ移行する。最新でないときはステップS160へ移行する(ステップS150)。

【0150】最新と判断されたとき、暗号処理部328は、暗号処理部326から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8をライセンス管理デバイス520において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を通信装置350を介してパーソナルコンピュータ50へ送信する(ステップS152)。

【0151】そして、パーソナルコンピュータ50のコントローラ510は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し(ステップS154)、バスBS5を介してライセンス管理デバイス520に入力する。ライセンス管理デバイス520の復号処理部5212は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を端子5226およびインタフェース5224を介して受取り、セッションキー発生部5218によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8を受信する(ステップS158)。その後、ステップS172へ移行する。

【0152】一方、最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラスリストのデータCRLdateを取得し、差分データである差分CRLを生成する(ステップS160)。

【0153】暗号処理部328は、暗号処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの差分CRLとを受けて、ライセンス管理デバイス520において生成されたセッションキーKs2によって暗号化する。暗号処理部328より出力された暗号化データ{差分CRL//トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2は、バスBS1および通信装置350を介してパーソナルコンピュータ50に送信される(ステップS162)。

【0154】パーソナルコンピュータ50は、送信された暗号化データ{差分CRL//トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し(ステップS164)、バス

BS5を介してライセンス管理デバイス520に入力する(ステップS166)。ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2を用いてバスBS5の受信データを復号しバスBS5に出力する(ステップS168)。

【0155】この段階で、バスBS5には、Kmc保持部5221に保持される秘密復号鍵Kmc8で復号可能な暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}と、差分CRLとが出力される(ステップS168)。コントローラ5220の指示によって受理した差分CRLによってメモリ5215内のCRL領域5215Aを差分CRLに基づいて更新する(ステップS170)。

【0156】ステップS152、S154、S156、S158は、ライセンス管理デバイス520の禁止クラスリストCRLが最新の場合のライセンス鍵Kc等のライセンス管理デバイス520への配信動作であり、ステップS160、S162、S164、S166、S168、S170は、ライセンス管理デバイス520の禁止クラスリストCRLが最新でない場合のライセンス鍵Kc等のライセンス管理デバイス520への配信動作である。このように、ライセンス管理デバイス520から送られてきた禁止クラスリストCRLdateが更新されているか否かを、逐一、確認し、最新の禁止クラスリストCRLをCRLデータベース306から取得し、差分CRLをライセンス管理デバイス520に配信することによって、配信したライセンスが、クラス鍵等の破られた機器に対して出力され、流出することを防止できる。

【0157】ステップS158またはステップS170の後、コントローラ5220の指示によって、暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8は、復号処理部5204において、秘密復号鍵Kmc8によって復号され、ライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、再生回数制限ACmおよび再生期限ACp)が受理される(ステップS172)。

【0158】このように、配信サーバおよびライセンス管理デバイスでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【0159】図13を参照して、コントローラ510は、ライセンス管理デバイス520が受理したライセンスを格納するためのエントリ番号を、ライセンス管理デバイス520に入力する(ステップS174)。そうす

ると、ライセンス管理デバイス520のコントローラ5220は、端子5226およびインタフェース5224を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ5215のライセンス領域5215Bに、ステップS172において取得したライセンス（ライセンス鍵Kc、トランザクションID、コンテンツID、再生回数制限ACmおよび再生期限ACp）を格納する（ステップS176）。

【0160】パーソナルコンピュータ50のコントローラ510は、配信サーバ10から送られたトランザクションIDと、ライセンスの配信受理を配信サーバ10へ送信する（ステップS178）。

【0161】配信サーバ10は、トランザクションIDおよびライセンスの配信受理を受信し（ステップS180）、課金データベース302への課金データの格納、およびトランザクションIDの配信記録データベース308への記録が行われる（ステップS182）。

【0162】一方、パーソナルコンピュータ50においては、ステップS178の後、ライセンスのエントリ番号、トランザクションID、およびコンテンツIDを含むライセンス管理ファイルを生成し、HDD530に記録する（ステップS184）。そして、コントローラ510は、CD-ROMドライブ540がCD-ROMから読出したコンテンツファイル（{Dc} Kc, Dc-inf）をHDD530にコピーし（ステップS186）、HDD530に記録されているコンテンツリストファイルに受理したコンテンツを追記し（ステップS188）、全体の動作が終了する。

【0163】このようにして、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス50が正規の機器であること、同時に、クラス証明書Cm7とともに暗号化して送信できた公開暗号鍵Kpm7が有効であることを確認した上で、クラス証明書Cm7が禁止クラスリスト、すなわち、公開暗号鍵Kpm7による暗号化が破られたクラス証明書リストに記載されていないライセンス管理デバイスからの配信要求に対してのみコンテンツデータのライセンスを配信することができ、不正なライセンス管理デバイスへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【0164】なお、パーソナルコンピュータ50からUSBケーブル70を介してCD-ROM60から取得された暗号化コンテンツデータを受信し、メモリカード110に暗号化コンテンツデータを記録した携帯電話機100は、上記図9～図13に示すフローチャートに従って、配信サーバ10から携帯電話網を介してライセンスを受信してメモリカード110に記録する。ただし、携帯電話機100が配信サーバ10からライセンスを受信するときは、パーソナルコンピュータ50を介したCD-ROM60からの暗号化コンテンツデータの取得が最初に行われる。この場合は、最初に暗号化コンテンツデ

ータを受信しないと、携帯電話機100は、サーバ情報ファイルを取得できず、アクセスすべき配信サーバや、配信サーバとの接続手段が解らないからである。

【0165】【移動】図1に示すデータ配信システムにおいて、CD-ROM60から取得された暗号化コンテンツデータと、配信サーバ10からパーソナルコンピュータ50のライセンス管理デバイス520へ配信された暗号化コンテンツデータのライセンスを携帯電話機100に装着されたメモリカード110へ送信する動作について説明する。なお、この動作を「移動」という。

【0166】図14～図17は、図1に示すデータ配信システムにおいて、ライセンス管理デバイス520が配信サーバ10から受信した暗号化コンテンツデータのライセンスと、CD-ROM60から取得した暗号化コンテンツデータを携帯電話機100に装着されたメモリカード110へ移動する移動動作を説明するための第1～第4のフローチャートである。

【0167】図14を参照して、パーソナルコンピュータ50のキーボード560から移動リクエストが入力されると（ステップS300）、コントローラ510は、認証データの送信要求をUSBインタフェース550、端子580、およびUSBケーブル70を介して携帯電話機100へ送信する（ステップS302）。そうすると、携帯電話機100のコントローラ1106は、端子1114、USBインタフェース1112およびバスBS3を介して認証データの送信要求を受信し、バスBS3およびメモリカードインタフェース1200を介して認証データの送信要求をメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する（ステップS304）。

【0168】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ{Kpm3//Cm3}KPaをバスBS4を介して読出し、その読出した認証データ{Kpm3//Cm3}KPaをバスBS4、インタフェース1424および端子1426を介して携帯電話機100へ出力する。そして、携帯電話機100のコントローラ1106は、メモリカードインタフェース1200およびバスBS3を介して認証データ{Kpm3//Cm3}KPaを受取り、バスBS3、USBインタフェース1112、端子1114およびUSBケーブル70を介してパーソナルコンピュータ50へ認証データ{Kpm3//Cm3}KPaを送信する（ステップS306）。

【0169】そうすると、パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して認証データ{Kpm3//Cm3}KPaを受信し（ステップS308）、その受信した認証データ{Kpm3//Cm3}KPaをバスB

S 2を介してライセンス管理デバイス520へ送信する。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介して認証データ{K P m 3 / / C m 3} K P aを受信し、その受信した認証データ{K P m 3 / / C m 3} K P aを復号処理部5208へ与える。認証処理部5208は、K P a保持部5214からの認証鍵K P aによって認証データ{K P m 3 / / C m 3} K P aの復号処理を実行する(ステップS 310)。コントローラ5220は、復号処理部5208における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからの公開暗号鍵K P m 3と証明書C m 3とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう(ステップS 312)。正当な認証データであると判断された場合、コントローラ5220は、公開暗号鍵K P m 3および証明書C m 3を承認し、受理する。そして、次の処理(ステップS 314)へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵K P m 3および証明書C m 3を受理しないで処理を終了する(ステップS 404)。

【0170】認証の結果、正規のメモリカードであることが認識されると、コントローラ5220は、次に、メモリカード110のクラス証明書C m 3が禁止クラスリストC R Lにリストアップされているかどうかをメモリ5215のC R L領域5215Aに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する(ステップS 404)。

【0171】一方、メモリカード110のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する(ステップS 314)。

【0172】認証の結果、正当な認証データを持つメモリカードを備える携帯電話機からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス520において、コントローラ5220は、移動を特定するための管理コードであるトランザクションIDをメモリ5215のライセンス領域5215Bから取得する(ステップS 316)。そして、セッションキー発生部5218は、移動のためのセッションキーK s 22を生成する(ステップS 318)。セッションキーK s 22は、復号処理部5208によって得られたメモリカード110に対応する公開暗号鍵K P m 3によって、暗号処理部5210によって暗号化される(ステップS 320)。コントローラ5220は、バスBS5を介して暗号化データ{K s 22} K m 3を取得し、メモリ5215から取得したトランザクションIDを暗号化データ{K s 22} K m 3に追加し、たトランザクションID / / {K s 22} K m 3をバス

BS5、インタフェース5224および端子5226を介して出力する(ステップS 322)。

【0173】図15を参照して、パーソナルコンピュータ50のコントローラ510は、バスBS2を介してトランザクションID / / {K s 22} K m 3を受信し(ステップS 324)、USBインタフェース550、端子580、およびUSBケーブル70を介してトランザクションID / / {K s 22} K m 3を携帯電話機100へ送信する(ステップS 324)。そうすると、携帯電話機100のコントローラ1106は、端子1114、USBインタフェース1112、およびBS3を介してトランザクションID / / {K s 22} K m 3を受信し、その受信したトランザクションID / / {K s 22} K m 3をメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介してトランザクションID / / {K s 22} K m 3を受信する(ステップS 326)。復号処理部1422は、コントローラ1420からバスBS4を介して{K s 22} K m 3を受取り、K m保持部1421からの秘密復号鍵K m 3によって{K s 22} K m 3を復号してセッションキーK s 22を受理する(ステップS 328)。そして、セッションキー発生部1418は、セッションキーK s 22を生成し(ステップS 330)、コントローラ1420は、バスBS4を介してメモリ1415のC R L領域1415Aから禁止クラスリストの更新日時C R L d a t eを取得し、その取得した更新日時C R L d a t eを切換スイッチ1446へ与える(ステップS 332)。

【0174】そうすると、暗号処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーK s 2、公開暗号鍵K P m c 4および禁止クラスリストC R L d a t eを、復号処理部1404によって復号されたセッションキーK s 22によって暗号化し、暗号化データ{K s 2 / / K P m c 4 / / C R L d a t e} K s 22を生成する。コントローラ1420は、暗号化データ{K s 2 / / K P m c 4 / / C R L d a t e} K s 22をバスBS4、インタフェース1424および端子1426を介して携帯電話機100へ出力し、携帯電話機100のコントローラ1106は、メモリカードインタフェース1200を介して暗号化データ{K s 2 / / K P m c 4 / / C R L d a t e} K s 22を受取る。そして、コントローラ1106は、USBインタフェース1112、端子1114、およびUSBケーブル70を介してパーソナルコンピュータ50へ送信する(ステップS 334)。

【0175】パーソナルコンピュータ50のコントローラ510は、端子580およびUSBインタフェース550を介して暗号化データ{K s 2 / / K P m c 4 / /

CRLdate) Ks22を受信し(ステップS336)、バスBS2を介して暗号化データ{Ks2//KPmc4//CRLdate) Ks22をライセンス管理デバイス520へ入力する(ステップS338)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224およびバスBS5を介して暗号化データ{Ks2//KPmc4//CRLdate) Ks22を受信し、その受信した暗号化データ{Ks2//KPmc4//CRLdate) Ks22を復号処理部5212に与える。復号処理部5212は、セッションキー発生部5218からのセッションキーKs22によって暗号化データ{Ks2//KPmc4//CRLdate) Ks22を復号し、セッションキーKs2、公開暗号鍵KPmc4および禁止クラスリストの更新日時CRLdateを受信する(ステップS340)。

【0176】そうすると、パーソナルコンピュータ50のコントローラ510は、ステップS324においてライセンス管理デバイス520から取得したトランザクションIDに基づいて、HDD530に記録されたコンテンツリストファイルに含まれるライセンス管理ファイルを検索し、取得したトランザクションIDが含まれるライセンス管理ファイルと同じライセンス管理ファイルに含まれるライセンスのエントリ番号をHDD530から読出す。そして、コントローラ510は、その読出したエントリ番号をバスBS2を介してライセンス管理デバイス520へ入力する(ステップS342)。ライセンス管理デバイス520のコントローラ5220は、端子5226、インタフェース5224、およびバスBS5を介してエントリ番号を受信し、メモリ5215のライセンス領域5215Bにおいて受信したエントリ番号によって指定された領域からトランザクションID、コンテンツID、ライセンス鍵Kc、再生回数制限ACm、再生期限ACpを読出す(ステップS344)。

【0177】再生回数制限ACmの受理に応じて、コントローラ5220は、再生回数制限ACmを確認する(ステップS346)。つまり、コントローラ5220は、取得した再生回数制限ACmに基づいて、携帯電話機100に装着されたメモリカード110へ移動しようとするライセンスが再生回数制限ACmによって暗号化コンテンツデータの再生ができないライセンスになっているか否かを確認する。再生回数が再生回数制限ACmによる制限回数に達している場合、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを携帯電話機100に装着されたメモリカード110へ移動する意味がないからである。

【0178】ステップS346において、暗号化コンテンツデータの再生回数が再生回数制限ACmによる制限回数に達していた場合、ステップS404へ移行し、移

動動作は終了する。ステップS346において、暗号化コンテンツデータの再生回数が再生回数制限ACmによる制限回数に達していない場合、ステップS348へ移行する。

【0179】図16を参照して、暗号処理部5217は、復号処理部5212によって得られたライセンス管理デバイス520固有の公開暗号鍵KPmc4によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4を生成する(ステップS348)。そして、メモリカード110から送信された禁止クラスリストの更新日時CRLdateによって、メモリカード110とライセンス管理デバイス320の保持する禁止クラスリストCRLのいずれが新しいかが判断され、メモリカード110が保持する禁止クラスリストが新しいか同じと判断されたとき、ステップS350へ移行する。また、ライセンス管理デバイス520が保持する禁止クラスリストが最新でないときはステップS362へ移行する(ステップS350)。

【0180】メモリカード110の方が新しい、もしくは、同じと判断されたとき、暗号処理部5206は、暗号処理部5217から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4をセッションキー発生部5218において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4} Ks2をバスBS5に出力する。そして、コントローラ5220は、バスBS5上の暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4} Ks2をインタフェース5224および端子5226を介してパーソナルコンピュータ50へ送信する(ステップS352)。そして、コントローラ5220は、メモリ5215のライセンス領域5215Bにおいて指定されたエントリ番号内のライセンスを削除する(ステップS354)。

【0181】パーソナルコンピュータ50のコントローラ510は、暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4} Ks2を受取り、USBインタフェース550、端子580、およびUSBケーブル70を介して携帯電話機100へ送信する(ステップS356)。

【0182】携帯電話機100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4} Ks2を受信し、その受信した暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp) Km c4} Ks2をバスBS3およびメモリカードインタフェース1200を介

してメモ리카ード110へ送信する。そして、メモ리카ード110のコントローラ1420は、端子1426、端子1424、およびバスBS4を介して暗号化データ { {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受信する (ステップS358)。

【0183】メモ리카ード110の復号処理部1412は、暗号化データ { {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2をバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4を受理する (ステップS360)。その後、図17に示すステップS376へ移行する。

【0184】一方、ステップS350において、ライセンス管理デバイスの方が新しいと判断されると、ライセンス管理デバイス520のコントローラ5220は、バスBS5を介してメモリ5215のCRL領域5215Aから最新の禁止クラスリストのデータCRLを取得する (ステップS362)。

【0185】暗号処理部5206は、暗号処理部5217の出力と、コントローラ5220がバスBS5を介してメモリ5215から取得した禁止クラスリストのデータCRLとを、それぞれ、切換スイッチ5242および5246を介して受取り、セッションキー発生部5218において生成されたセッションキーKs2によって暗号化する。暗号処理部5206より出力された暗号化データ {CRL// {トランザクションID//コンテンツID//インタフェース5224、および端子5226を介してパーソナルコンピュータ50に出力される (ステップS364)。そして、コントローラ5220は、メモリ5215のライセンス領域5215Bにおける指定されたエントリ番号内のライセンスを削除する (ステップS366)。

【0186】このように、ライセンス管理デバイスおよびメモ리카ードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスの移動動作におけるセキュリティを向上させることができる。

【0187】パーソナルコンピュータ50のコントローラ510は、出力された暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受信し、USBインタフェース550、端子580、およびUSBケーブル70を介して暗号化データ {CRL// {トランザク

ACp} Kmc4} Ks2を携帯電話機100へ送信する (ステップS368)。携帯電話機100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受取り、バスBS3およびメモ리카ードインタフェース1200を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2をメモ리카ード110へ送信する。そして、メモ리카ード110のコントローラ1420は、端子1426、インタフェース1424、およびバスBS4を介して暗号化データ {CRL// {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4} Ks2を受信する (ステップS370)。

【0188】メモ리카ード110において、復号処理部1412は、セッションキー発生部1418から与えられたセッションキーKs2を用いてバスBS4上の受信データを復号し、CRLと {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4とを受理する (ステップS372)。コントローラ1420は、復号処理部1412によって受理されたデータCRLをバスBS4を介して受取り、その受取ったデータCRLによってメモリ1415のCRL領域1415Aを書換える (ステップS374)。

【0189】ステップS352、S354、S356、S358、S360は、メモ리카ード110の保持する禁止クラスリストCRLが、ライセンス管理デバイス520の禁止クラスリストCRLより新しいか、同じ場合のライセンス鍵Kc等のメモ리카ード110への移動動作であり、ステップS362、S364、S366、S368、S370、S372、S374は、メモ리카ード110の保持する禁止クラスリストCRLが、ライセンス管理デバイス520の禁止クラスリストCRLより古い場合のライセンス鍵Kc等のメモ리카ード110への移動動作である。このように、メモ리카ード110から送られてきた禁止クラスリストの更新日時CRLdateに従って、逐一、確認し、より最新の禁止クラスリストCRLに更新される。を防止できる。

【0190】図17を参照して、ステップS360またはステップS374の後、コントローラ1420の指示によって、暗号化ライセンス {トランザクションID//コンテンツID//Kc//ACm//ACp} Kmc4は、復号処理部1404において、秘密復号鍵Kmc4によって復号され、ライセンス (ライセンス鍵Kc、トランザクションID、コンテンツID、再生回数制限ACmおよび再生期限ACp) が受理される (ステップS376)。

【0191】パーソナルコンピュータ50のコントロー

ラ510は、メモリカード110へ移動したライセンスを格納するためのエントリ番号を、USBインタフェース550、端子580、およびUSBケーブル70を介して携帯電話機100へ送信し、携帯電話機100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してエントリ番号を受取り、バスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信する

(ステップS378)。そうすると、メモリカード110のコントローラ1420は、端子1426およびインタフェース1424を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ステップS376において取得したライセンス(ライセンス鍵Kc、トランザクションID、コンテンツID、再生回数制限ACmおよび再生期限ACp)を格納する(ステップS380)。

【0192】パーソナルコンピュータ50のコントローラ510は、メモリカード110のメモリ1415に格納されたライセンスのエントリ番号と、平文のトランザクションIDおよびコンテンツIDを含むメモリカード110へ移動しようとする暗号化コンテンツデータ{Dc} Kcと付加情報Dc-infに対するライセンス管理ファイルを生成し、メモリカード110へ送信する(ステップS382)。

【0193】メモリカード110のコントローラ1420は、携帯電話機100を介してライセンス管理ファイルを受信し、メモリ1415のデータ領域1415Dに受信したライセンス管理ファイルを記録する(ステップS384)。

【0194】そして、パーソナルコンピュータ50のコントローラ510は、HDD530に記録されたライセンスのうち、メモリカード110へ移動したライセンスに対するライセンス管理ファイルをライセンス無に更新する(ステップS386)。その後、コントローラ510は、メモリカード110へ移動しようとする暗号化コンテンツデータ{Dc} Kcと付加情報Dc-infとをHDD530から取得し、{Dc} Kc//Dc-infをメモリカード110へ送信する(ステップS390)。メモリカード110のコントローラ1420は、携帯電話機100を介して{Dc} Kc//Dc-infを受信し(ステップS392)、バスBS4を介して受信した{Dc} Kc//Dc-infをメモリ1415のデータ領域1415Cに記録する(ステップS394)。

【0195】そうすると、パーソナルコンピュータ50のコントローラ510は、メモリカード110へ移動した楽曲を追記した再生リストを作成し(ステップS396)、再生リストと、再生リストの書換指示とをメモリカード110へ送信する(ステップS398)。メモリ

カード110のコントローラ1420は、携帯電話機100を介して再生リストと書換指示を受信し(ステップS400)、バスBS4を介してメモリ1415のデータ領域1415Cに記録されている再生リストを受信した再生リストに書換え(ステップS402)、移動動作が終了する(ステップS404)。

【0196】このようにして、携帯電話機100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵Kpm3が有効であることを確認した上で、クラス証明書Cm3が禁止クラスリスト、すなわち、公開暗号鍵Kpm3による暗号化が破られたクラス証明書リストに記載されていないメモリカードへの移動要求に対してのみコンテンツデータを移動することができ、不正なメモリカードへの移動および解読されたクラス鍵を用いた移動を禁止することができる。また、この移動動作を用いることによって、配信サーバ10との通信機能を有さない携帯電話機102のユーザも、パーソナルコンピュータ50を介して暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【0197】なお、上記においては、パーソナルコンピュータ50のライセンス管理デバイス520からメモリカード110へのライセンスの移動について説明したが、メモリカード110からライセンス管理デバイス520へのライセンスの移動も、図14～図17に示すフローチャートに従って行なわれる。

【0198】図18を参照して、パーソナルコンピュータ50のライセンス管理デバイス520によって受信されたライセンスの管理について説明する。パーソナルコンピュータ50のHDD530は、コンテンツリストファイル150と、コンテンツファイル1531～153nと、ライセンス管理ファイル1521～152nとを含む。

【0199】コンテンツリストファイルは、HDD530に記録されているコンテンツを管理するためのファイルで、コンテンツの一覧と、対応するコンテンツファイルとライセンス管理ファイルへの関係を示す情報ファイルである。

【0200】コンテンツファイル1531～153nは、CD-ROMから取得された暗号化コンテンツデータ{Dc} Kcと付加情報Dc-infとが記録されたファイルである。なお、コンテンツファイル1531～153nは、CD-ROMに記録されているコンテンツファイル601～60nのコピーである。また、ライセンス管理ファイル1521～152nは、それぞれ、コンテンツファイル1531～153nに対応して記録されており、ライセンス管理デバイス520によって受信されたライセンスを管理する。

【0201】ライセンス管理ファイル1521、152

4は、それぞれ、エントリ番号0、2を含む。これは、ライセンス管理デバイス520によって受信され、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Bにおいて管理されるライセンス（ライセンスID、ライセンス鍵Kc、再生回数制限ACmおよび再生期限ACm）の管理領域を指定する番号である。

【0202】したがって、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを携帯電話機100に装着されたメモリカード110へ移動させると、コンテンツファイル1531～153nを検索してコンテンツファイル1531を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル1531に対応するライセンス管理ファイル1521に含まれるエントリ番号は「0」であるので、コンテンツファイル1531に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス520のメモリ5215のライセンス領域5215Bのエントリ番号0によって指定された領域に記録されている。そうすると、HDD530に記録されたコンテンツリストファイル150のライセンス管理ファイル1521からエントリ番号0を読み出し、その読み出したエントリ番号0をライセンス管理デバイス520に入力することによって、メモリ5215のライセンス領域5215Bからライセンスを容易に取出し、メモリカード110へ移動できる。そして、ライセンスを移動した後、ライセンスの複製が禁止されているとき、メモリ5215のライセンス領域5215Bにおいて指定されたエントリ番号0内のライセンスは削除されるので、それに対応してライセンス管理ファイル1523のように「ライセンス無」が記録される。

【0203】図19は、メモリカード110のメモリ1415におけるデータ領域1415Cに記録された再生リストファイル160と、コンテンツファイル1611～161nと、ライセンス管理ファイル1621～162nとの関係を示したものである。再生リスト160は、パーソナルコンピュータ50におけるコンテンツリストファイル150に相当する情報リストであり、携帯電話機100ではこの再生リストを参照して、通常、リスト順に再生していく。コンテンツファイル1611～161nは、受信した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-infとのファイル名を記録する。また、ライセンス管理ファイル1621～162nは、それぞれ、コンテンツファイル1611～161nに対応して記録されている。

【0204】また、ライセンス管理ファイル1621～162nは、メモリ1415のライセンス領域1415Cに格納されたライセンスの領域を指定するためのエントリ番号を含む。したがって、ライセンス管理ファイル

1621～162nからエントリ番号を読み出せば、ライセンス管理ファイル1621～162nに対応する暗号化コンテンツデータを再生するライセンスがどの領域に格納されているのかが解り、容易にライセンスを取り出すことができる。

【0205】なお、ライセンス管理ファイル1622は、「ライセンス無」を表しているが、これは、たとえば、携帯電話機100が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当し、暗号化コンテンツデータはメモリ1415に存在するが、その暗号化コンテンツデータを再生するライセンスが存在しないことを意味する。

【0206】[再生] 次に、図20および図21を参照してメモリカード110に記録されたコンテンツデータの携帯電話機100（コンテンツ再生デバイスとも言う、以下同じ）における再生動作について説明する。図20を参照して、再生動作の開始とともに、携帯電話機100のユーザから操作パネル1108を介して再生指示が携帯電話機100にインプットされる（ステップS1000）。そうすると、コントローラ1106は、バスBS3を介して認証データ保持部1500から認証データ{Kp1//Cp1}Kpaを読み出し、メモリカードインタフェース1200を介してメモリカード110へ認証データ{Kp1//Cp1}Kpaを出力する（ステップS1002）。

【0207】そうすると、メモリカード110は、認証データ{Kp1//Cp1}Kpaを受信する（ステップS1004）。そして、メモリカード110の復号処理部1408は、受信した認証データ{Kp1//Cp1}Kpaを、Kpa保持部1414に保持された公開認証鍵Kpaによって復号し（ステップS1006）、コントローラ1420は復号処理部1408における復号処理結果から、認証処理を行なう。すなわち、認証データ{Kp1//Cp1}Kpaが正規の認証データであるか否かを判断する認証処理を行なう（ステップS1008）。復号できなかった場合、ステップS1048へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ1420は、取得したクラス証明書Cp1がメモリ1415から読み出した禁止クラスリストデータCRLに含まれるか否かを判断する（ステップS1010）。この場合、クラス証明書Cp1にはIDが付与されており、コントローラ1420は、受信したクラス証明書Cp1のIDが禁止クラスリストデータの中に存在するか否かを判別する。クラス証明書Cp1が禁止クラスリストデータに含まれると判断されると、ステップS1048へ移行し、再生動作は終了する。

【0208】ステップS1010において、証明書Cm1が禁止クラスリストデータCRLに含まれていないと判断されると、メモリカード110のセッションキー発

生部1418は、再生セッション用のセッションキーKs2を発生させる(ステップS1012)。そして、暗号処理部1410は、セッションキー発生部1418からのセッションキーKs2を、復号処理部1408で復号された公開暗号鍵Kp1によって暗号化した{Ks2}Kp1をバスBS3へ出力する(ステップS1014)。そうすると、コントローラ1420は、インタフェース1424および端子1426を介してメモリカードインタフェース1200へ{Ks2}Kp1を出力する(ステップS1016)。携帯電話機100のコントローラ1106は、メモリカードインタフェース1200を介して{Ks2}Kp1を取得する。そして、Kp1保持部1502は、秘密復号鍵Kp1を復号処理部1504へ出力する。

【0209】復号処理部1504は、Kp1保持部1502から出力された、公開暗号鍵Kp1と対になっている秘密復号鍵Kp1によって{Ks2}Kp1を復号し、セッションキーKs2を暗号処理部1506へ出力する(ステップS1018)。そうすると、セッションキー発生部1508は、再生セッション用のセッションキーKs3を発生させ、セッションキーKs3を暗号処理部1506へ出力する(ステップS1020)。暗号処理部1506は、セッションキー発生部1508からのセッションキーKs3を復号処理部1504からのセッションキーKs2によって暗号化して{Ks3}Ks2を出力し、コントローラ1106は、バスBS3およびメモリカードインタフェース1200を介して{Ks3}Ks2をメモリカード110へ出力する(ステップS1022)。

【0210】そうすると、メモリカード110の復号処理部1412は、端子1426、インタフェース1424、およびバスBS4を介して{Ks3}Ks2を入力する(ステップS1024)。

【0211】図21を参照して、復号処理部1412は、セッションキー発生部1418によって発生されたセッションキーKs2によって{Ks3}Ks2を復号して、携帯電話機100で発生されたセッションキーKs3を受理する(ステップS1026)。

【0212】再生端末のコントローラ1106は、メモリカード110から事前に取得したライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース1200を介してメモリカード110へ取得したエントリ番号を出力する(ステップS1027)。

【0213】エントリ番号が入力に応じて、コントローラ1420は、ライセンス領域1514Bの入力されたエントリの再生回数制限ACmを確認する(ステップS1028)。ステップS1028においては、メモリのアクセスに対する制限に関する情報である再生回数制限ACmを確認することにより、既に再生不可の状態であ

る場合には再生動作を終了し、再生回数制限に制限がある場合には再生回数制限ACmのデータを更新し再生可能回数を更新した後に次のステップに進む(ステップS1030)。一方、再生回数制限ACmによって再生回数が制限されていない場合においては、ステップS1030はスキップされ、再生回数制限ACmは更新されることなく処理が次のステップ(ステップS1032)に進行される。

【0214】ステップS1028において、当該再生動作において再生が可能であると判断された場合には、メモリ1415のライセンス領域1415Cに記録された再生リクエスト曲のライセンス鍵Kcおよび再生期限ACpがバスBS4上に出力される(ステップS1032)。

【0215】得られたライセンス鍵Kcと再生期限ACpは、切換スイッチ1446の接点Pfを介して暗号処理部1406に送られる。暗号処理部1406は、切換スイッチ1442の接点Pbを介して復号処理部1412より受けたセッションキーKs3によって切換スイッチ1446を介して受けたライセンス鍵Kcと再生期限ACpとを暗号化し、{Kc//ACp}Ks3をバスBS4に出力する(ステップS1034)。

【0216】バスBS4に出力された暗号化データは、インタフェース1424、端子1426、およびメモリカードインタフェース1200を介して携帯電話機100に送出される。

【0217】携帯電話機100においては、メモリカードインタフェース1200を介してバスBS3に伝達される暗号化データ{Kc//ACp}Ks3を復号処理部1510によって復号処理を行ない、ライセンス鍵Kcおよび再生期限ACpを受理する(ステップS1036)。復号処理部1510は、ライセンス鍵Kcを復号処理部1516に伝達し、再生期限ACpをバスBS3に出力する。

【0218】コントローラ1106は、バスBS3を介して、再生期限ACpを受理して再生の可否の確認を行なう(ステップS1040)。

【0219】ステップS1040においては、再生期限ACpによって再生不可と判断される場合には、再生動作は終了される。

【0220】ステップS1040において再生可能と判断された場合、コントローラ1106は、メモリカードインタフェース1200を介してメモリカード110に暗号化コンテンツデータ{Dc}Kcを要求する。そうすると、メモリカード110のコントローラ1420は、メモリ1415から暗号化コンテンツデータ{Dc}Kcを取得し、バスBS4、インタフェース1424、および端子1426を介してメモリカードインタフェース1200へ出力する(ステップS1042)。

【0221】携帯電話機100のコントローラ1106

は、メモリカードインタフェース1200を介して暗号化コンテンツデータ{Dc}Kcを取得し、バスBS3を介して暗号化コンテンツデータ{Dc}Kcを復号処理部1516へ与える。

【0222】そして、復号処理部1516は、暗号化コンテンツデータ{Dc}Kcを復号処理部1510から出力されたコンテンツ鍵Kcによって復号してコンテンツデータDataを取得する(ステップS1044)。

【0223】そして、復号されたコンテンツデータDcは音楽再生部1518へ出力され、音楽再生部1518は、コンテンツデータを再生し、DA変換器1519はデジタル信号をアナログ信号に変換して端子1530へ出力する。そして、音楽データは端子1530から外部出力装置を介してヘッドホーン130へ出力されて再生される(ステップS1046)。これによって再生動作が終了する。

【0224】上記においては、メモリカード110に記録された暗号化コンテンツデータを携帯電話機100によって再生する場合について説明したが、パーソナルコンピュータ50のコンテンツ再生デバイス1550は、HDD530に記憶された暗号化コンテンツデータをライセンス管理デバイス520に格納されたライセンスによって再生することができるが、その時の動作は図20および図21に示すフローチャートに従って行われる。

【0225】上記においては、CD-ROM60から暗号化コンテンツデータを取得したパーソナルコンピュータ50は、配信サーバ10から暗号化コンテンツデータを再生するライセンスを受信し、暗号化コンテンツデータとライセンスとを携帯電話機100に装着されたメモリカード110に移動する移動セッションについて説明した。したがって、本発明においては、図22に示すデータ配信システムも可能である。

【0226】すなわち、パーソナルコンピュータ50がCD-ROM60から暗号化コンテンツデータとサーバ情報ファイルとを取得し、その取得したサーバ情報ファイルに基づいて配信サーバ10に接続し、配信サーバ10からライセンスを受信する点は、図1に示すデータ配信システムと同じである。図22においては、パーソナルコンピュータ50は、取得した暗号化コンテンツデータおよびライセンスをUSBケーブル70、71を介して端末装置120、121へ移動する。

【0227】端末装置120、121は、データを配信サーバ10との間で送受信する通信機能を有しない端末装置であり、パーソナルコンピュータ50に内蔵されたライセンス管理デバイス520と同じ構成のデバイスが内蔵されている。そして、端末装置120、121は、パーソナルコンピュータ50から受信したライセンスを内蔵したデバイスに格納する。また、端末装置120、121は、暗号化コンテンツデータをハードディスク等に格納して管理する。さらに、端末装置120、121

は、上述したコンテンツ再生デバイス1550を内蔵しており、パーソナルコンピュータ50から受信した暗号化コンテンツデータを再生することも可能である。

【0228】図22に示すデータ配信システムによれば、配信サーバ10との通信機能を持たず、かつ、CD-ROM60から暗号化コンテンツデータを取得する機能も持たない端末装置であっても、CD-ROM60に記録された音楽データをライセンスとともに取得することができる。

【0229】本発明の実施の形態によれば、パーソナルコンピュータは音楽CDから暗号化コンテンツデータを取得する際、サーバへのアクセス手段やアクセス先を含むサーバ情報ファイルも取得するので、暗号化コンテンツデータの取得と同時に暗号化コンテンツデータを再生するライセンスを配信サーバから受信できる。

【0230】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図1】 本発明の実施の形態におけるデータ配信システムを概念的に説明する概略図である。

【図2】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図3】 図1に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図4】 図1に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図5】 図1に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図6】 図1に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図7】 図1に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図8】 図5に示すパーソナルコンピュータに内蔵されたライセンス管理デバイスの構成を示す概略ブロック図である。

【図9】 図1に示すデータ配信システムにおけるライセンスの配信動作を説明するための第1のフローチャートである。

【図10】 図1に示すデータ配信システムにおけるライセンスの配信動作を説明するための第2のフローチャートである。

【図11】 図1に示すデータ配信システムにおけるライセンスの配信動作を説明するための第3のフローチャートである。

【図12】 図1に示すデータ配信システムにおけるラ

イセンスの配信動作を説明するための第4のフローチャートである。

【図13】 図1に示すデータ配信システムにおけるライセンスの配信動作を説明するための第5のフローチャートである。

【図14】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第1のフローチャートである。

【図15】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第2のフローチャートである。

【図16】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第3のフローチャートである。

【図17】 図1に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第4のフローチャートである。

【図18】 パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

【図19】 メモリカードにおける再生リストファイルの構成を示す図である。

【図20】 携帯電話機における再生動作を説明するための第1のフローチャートである。

【図21】 携帯電話機における再生動作を説明するための第2のフローチャートである。

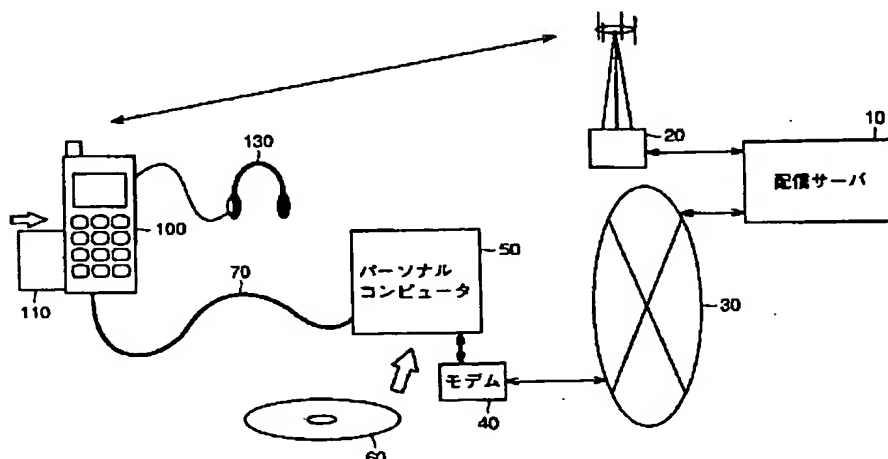
【図22】 本発明の実施の形態における他のデータ配信システムを概念的に説明する概略図である。

【符号の説明】

10 配信サーバ、20 配信キャリア、30 インターネット網、40 モデム、50、80 パーソナルコンピュータ、60 CD、70、71 USBケーブル、100 携帯電話機、110 メモリカード、120、121 端末装置、130 ヘッドホン、150

コンテンツリストファイル、160 再生リストファイル、302 課金データベース、304 情報データベース、306 CRLデータベース、307 メニューデータベース、308 配信記録データベース、310 データ処理部、312、320、1404、1408、1412、1422、1504、1510、1516、5204、5208、5212、5222 復号処理部、313 認証鍵保持部、315 配信制御部、316、セッションキー発生部、318、326、328、1406、1410、1417、1506、5206、5210、5217、5405 暗号処理部、350 通信装置、510、1106、1420、5220 コントローラ、511、811 ライセンス管理モジュール、520、820 ライセンス管理デバイス、530 ハードディスク、540 CD-ROMドライブ、550、1112 USBインタフェース、560 キーボード、570 ディスプレイ、580、1114、1426、1530、5226 端子、1108 操作パネル、1110 表示パネル、1200 メモリカードインタフェース、1400、1500、5200 認証データ保持部、1402、5202 Km c保持部、1414、5214 KPa保持部、1415、5215 メモリ、1415A、5215A CRL領域、1415B 再生リスト領域、1415C、5215B ライセンス領域、1415D データ領域、1416、5216 K P m c保持部、1418、5218 セッションキー発生部、1421、5221 Km保持部、1424、5224 インタフェース、1442、1446 切換スイッチ、1502 Kp 1保持部、1518 音楽再生部、1519 DA変換器、1521~152n、1621~162n ライセンス管理ファイル、1531~153n、1611~1612n コンテンツファイル、1550 コンテンツ再生デバイス。

【図1】



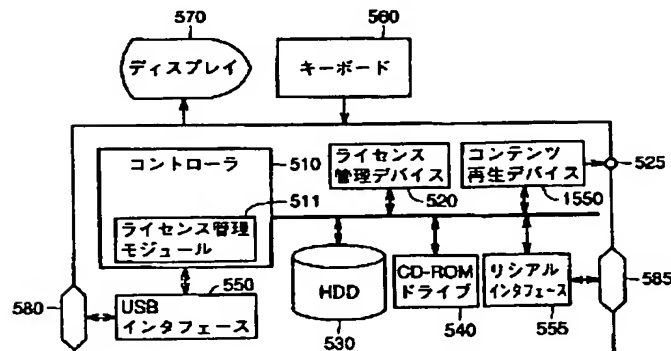
【図2】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ (Dc)Kcとして配信され、メモ리카ードに保持される
Dc-Inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス鍵 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID+コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止認証データのリスト CRLの更新日(CRLdate)を含む

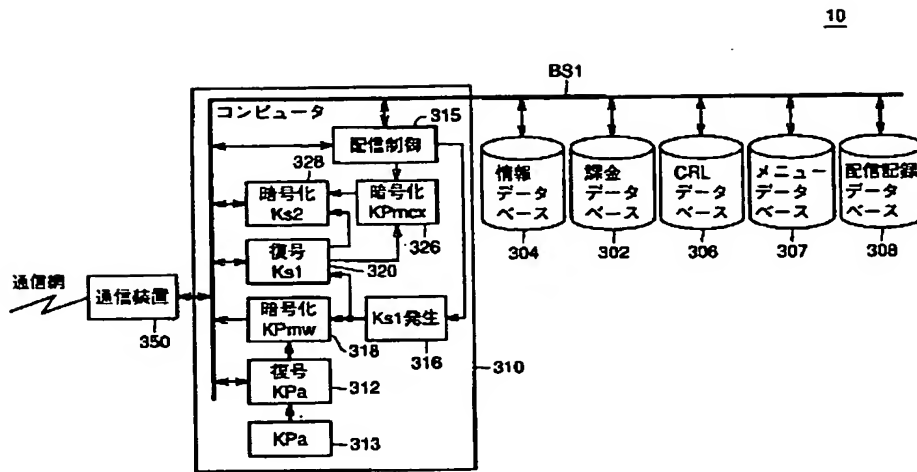
【図3】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション固有	メモ리카ードおよびコンテンツ管理モジュールと同一
メモ리카ード	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
ライセンス管理デバイス (ハードタンバ)	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモ리카ードごとに異なる。 xはモジュールを識別するための識別子
ライセンス管理モジュール (ソフトタンバ)	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール側のライセンスの授受ごとに発生
コンテンツ再生デバイス	Cmw	証明書	クラス証明書	メモ리카ード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。 {KPmw/Cmw}KPaの形式で出荷時に記録。 *メモ리카ード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスwごとに異なる。
	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール側の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 {KPpy/Cpy}KPaの形式で出荷時に記録。 *コンテンツ再生デバイスのクラスyごとに異なる。

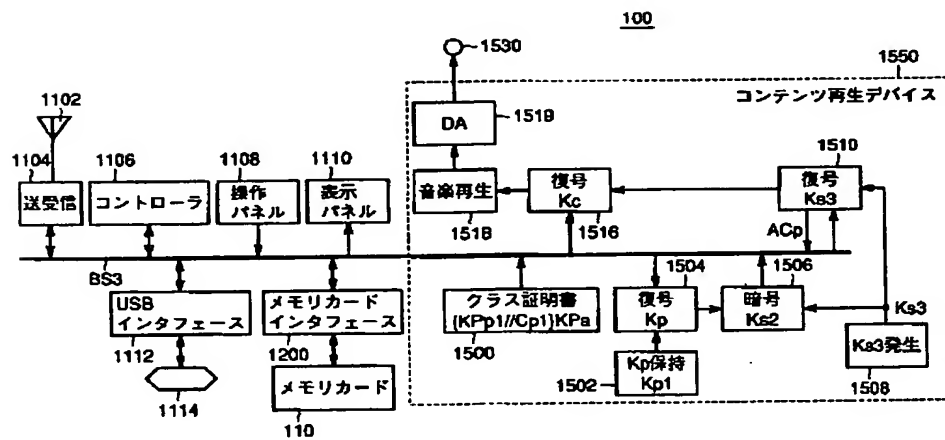
【図5】



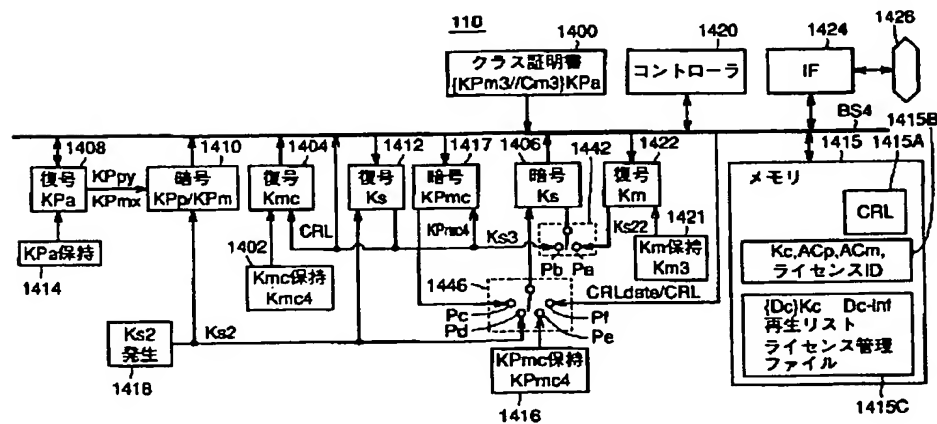
【図4】



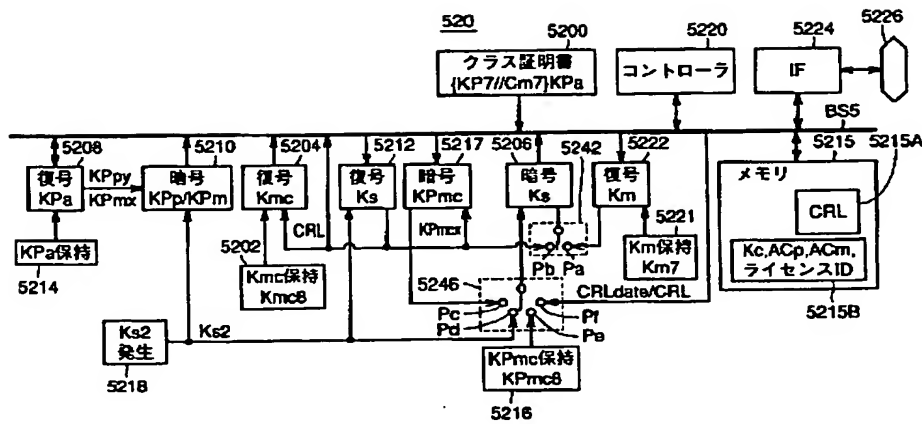
【図6】



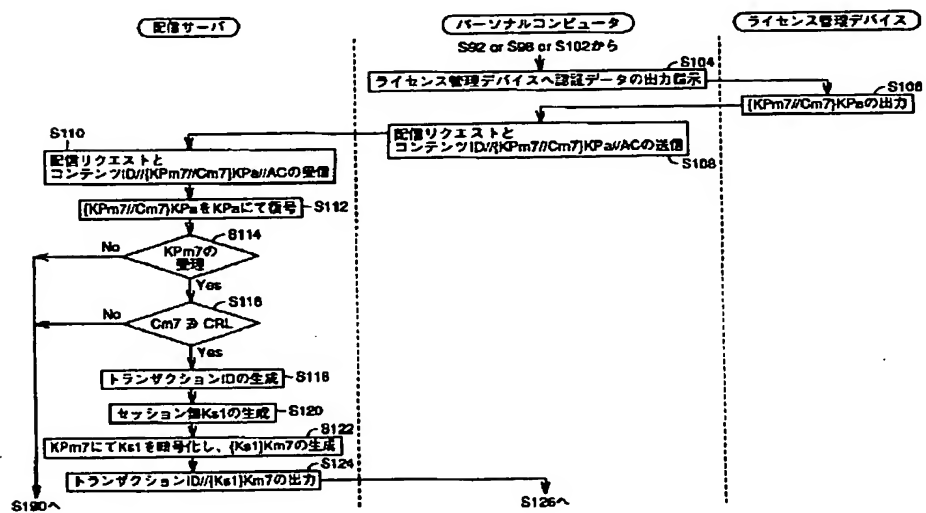
【図7】



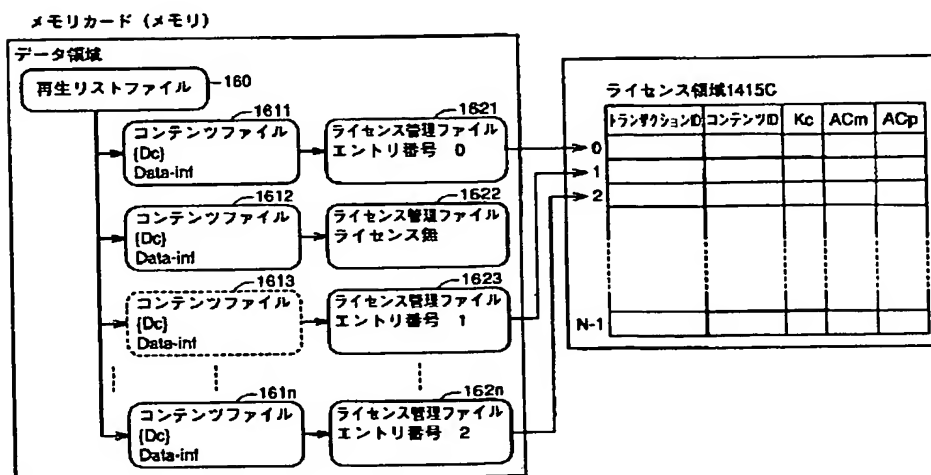
【図 8】



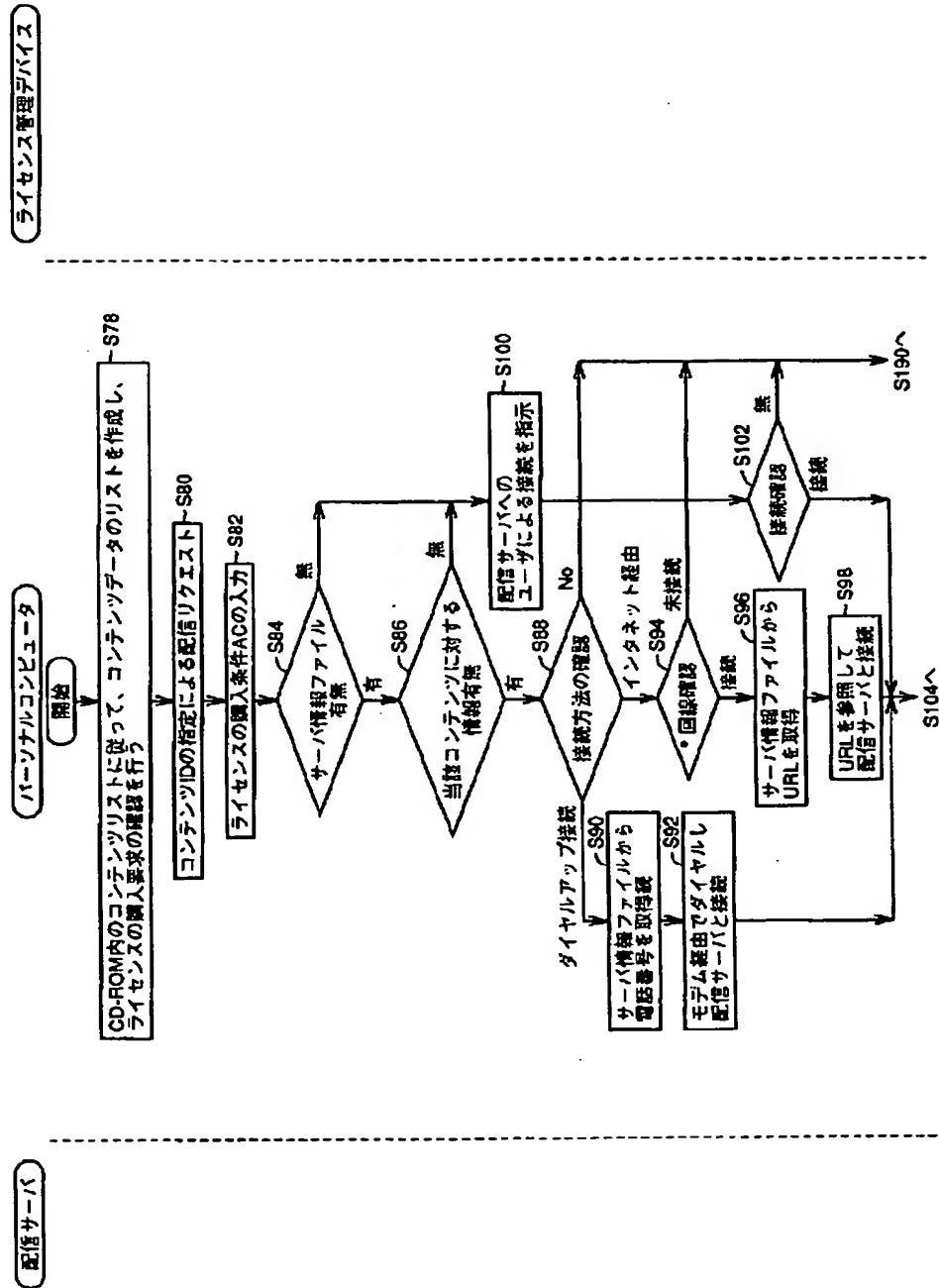
【図 10】



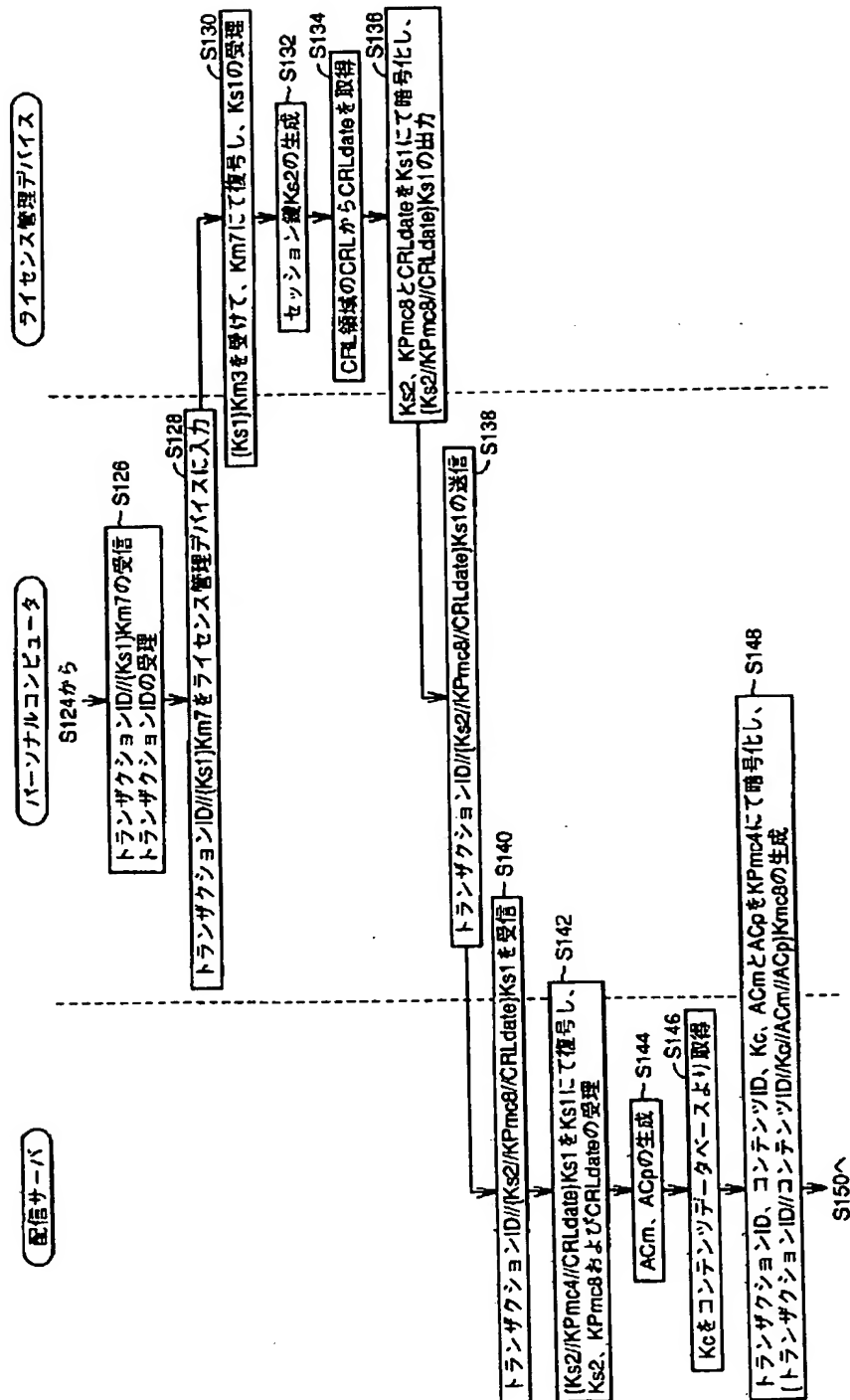
【図 19】



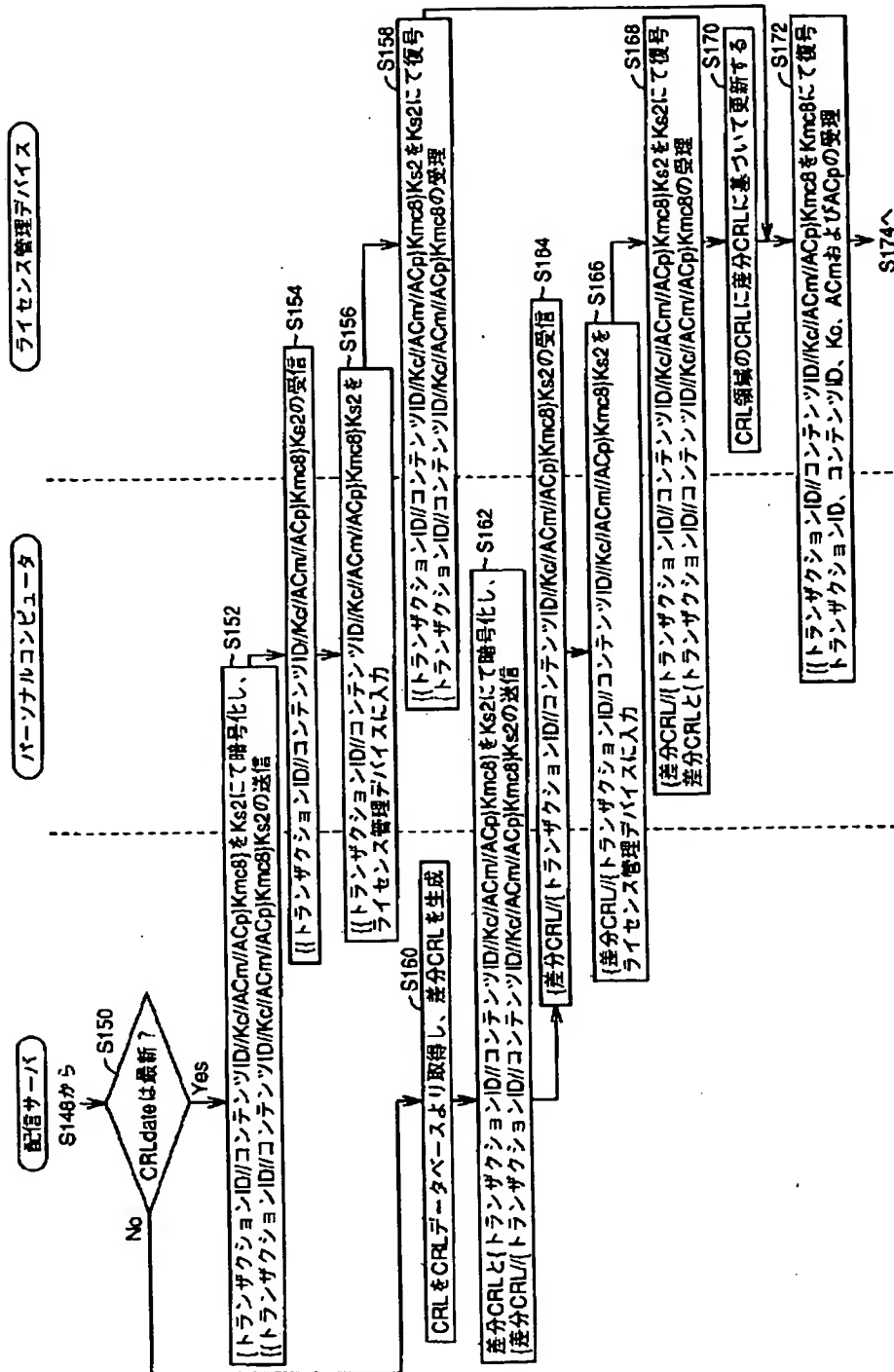
【図9】



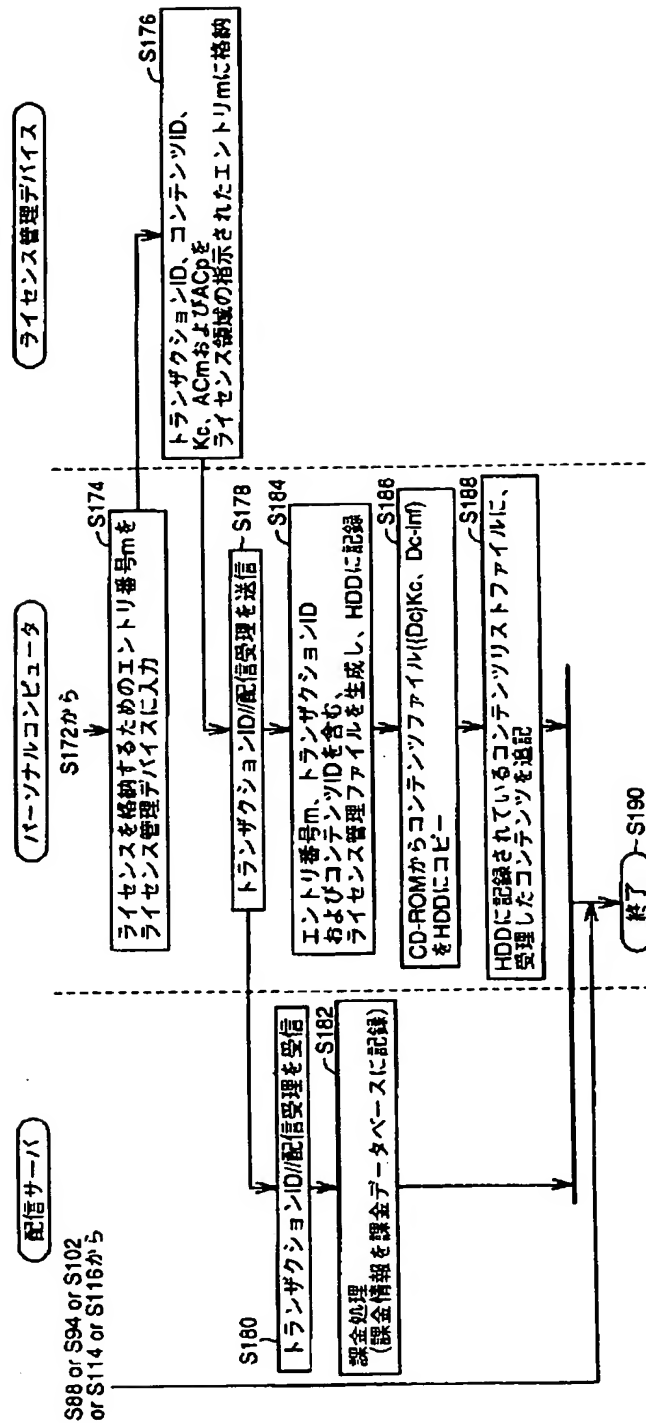
【図11】



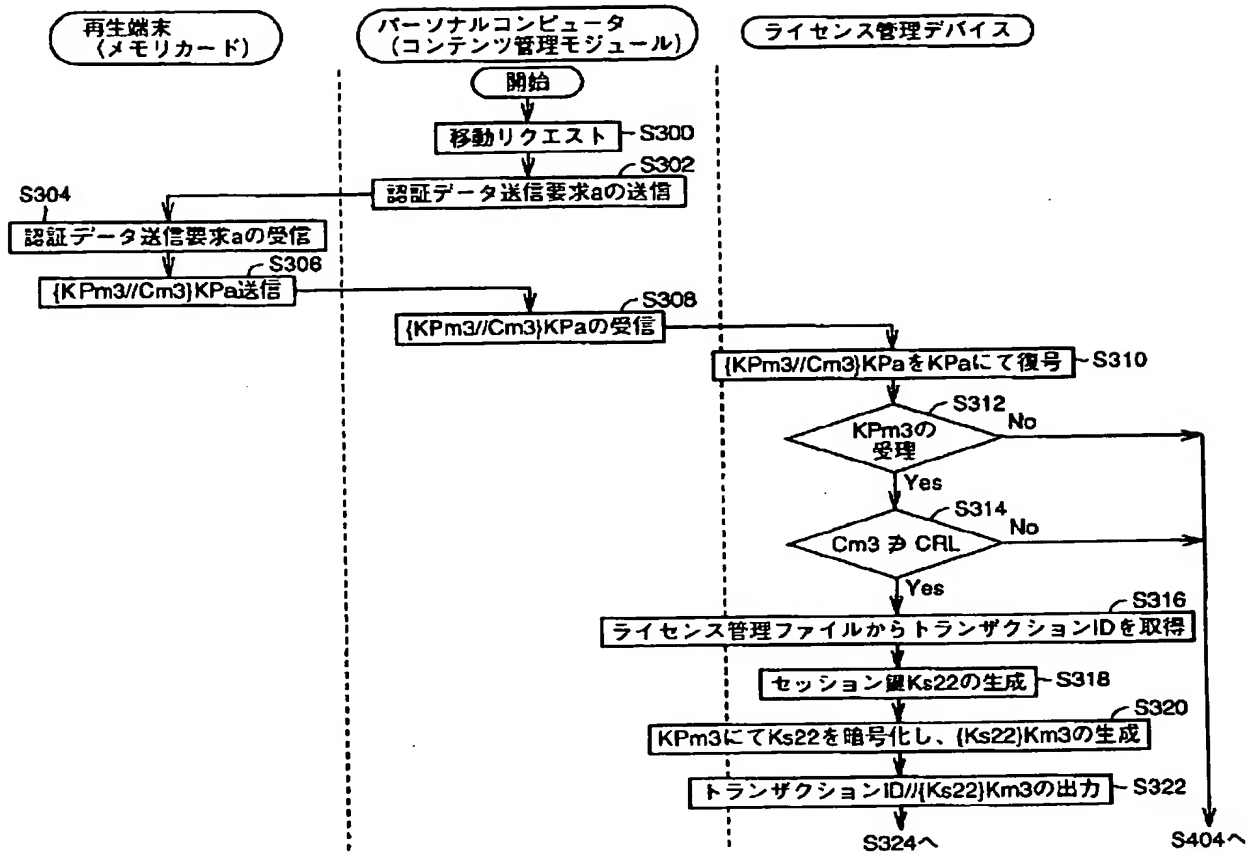
【図12】



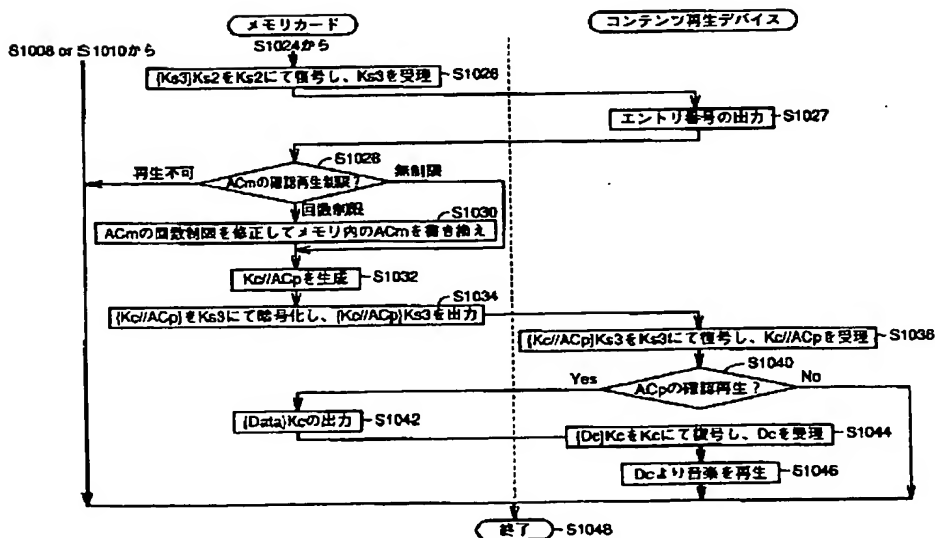
【図13】



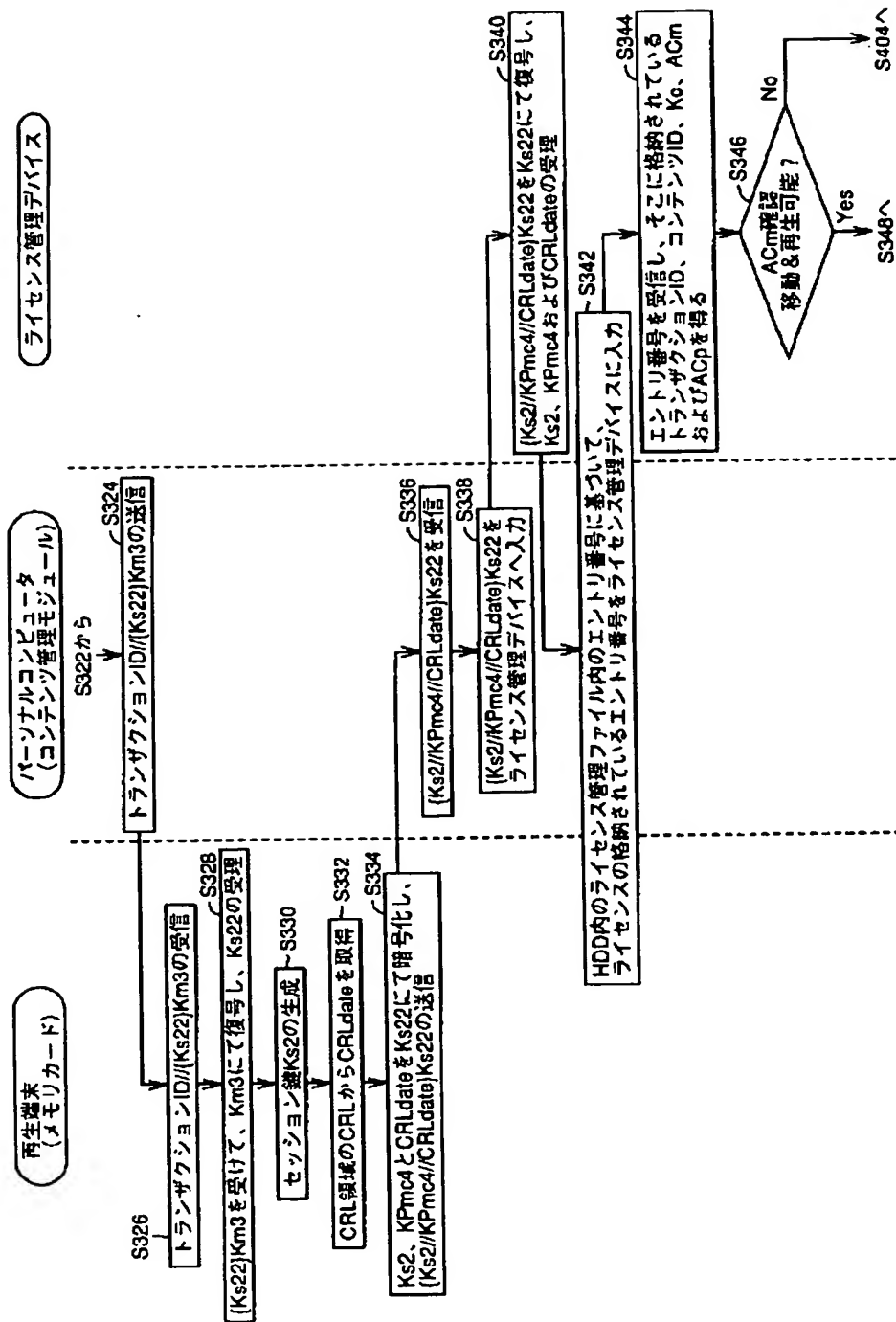
【図14】



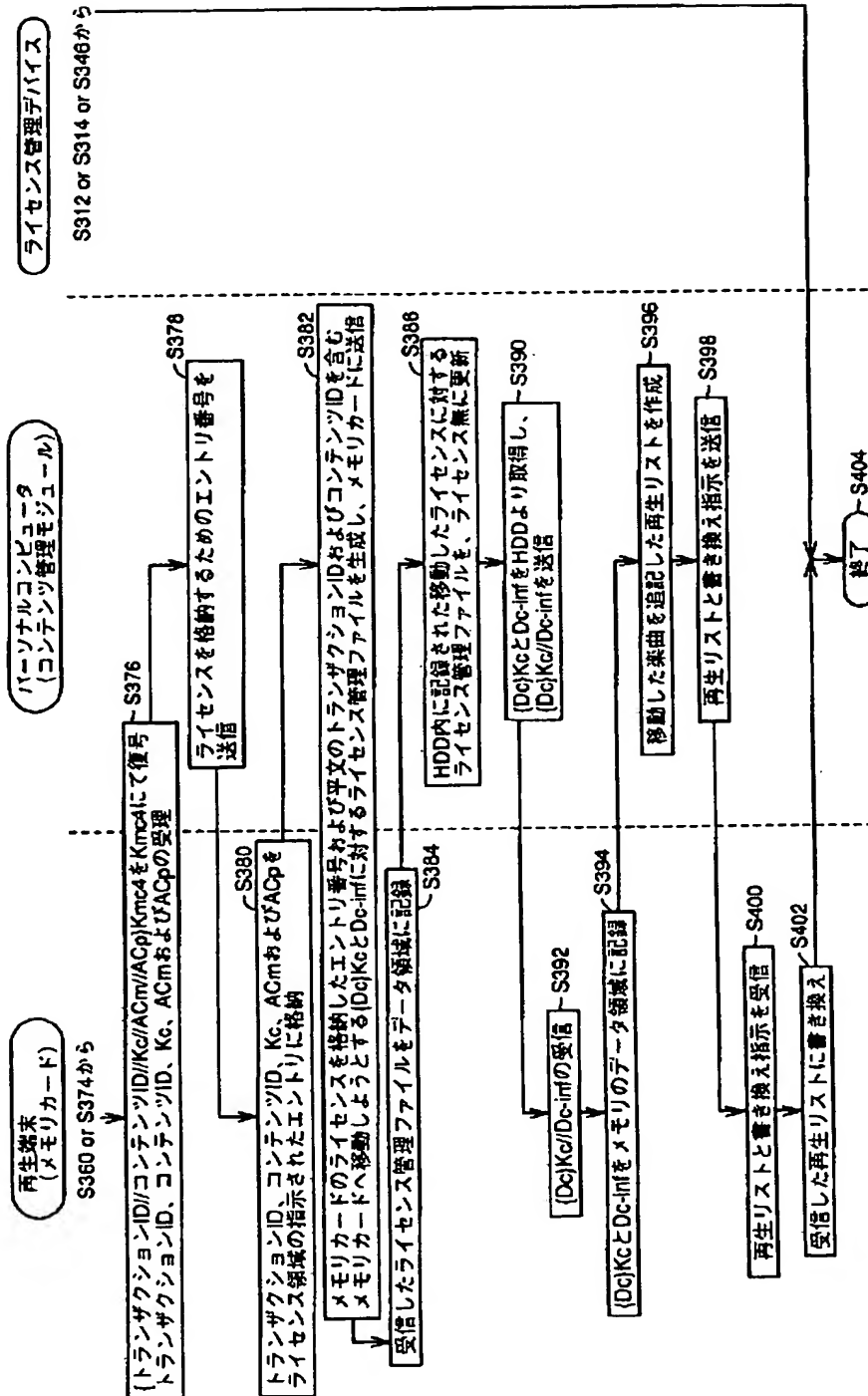
【図21】



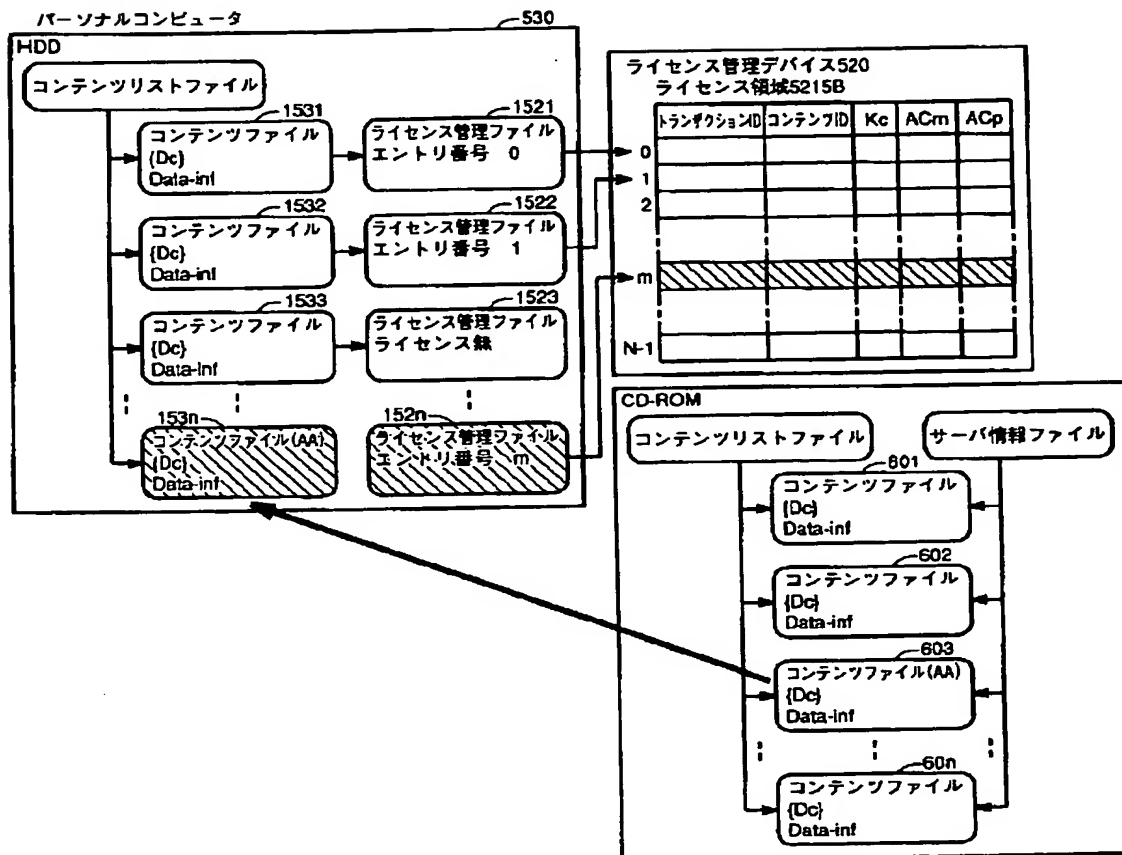
【図15】



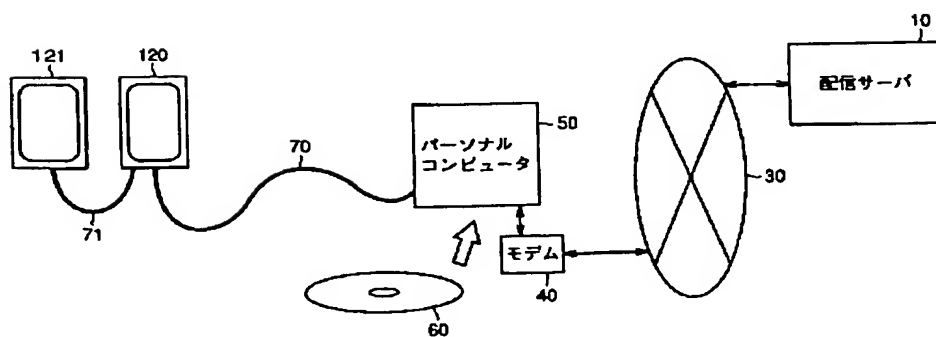
【図17】



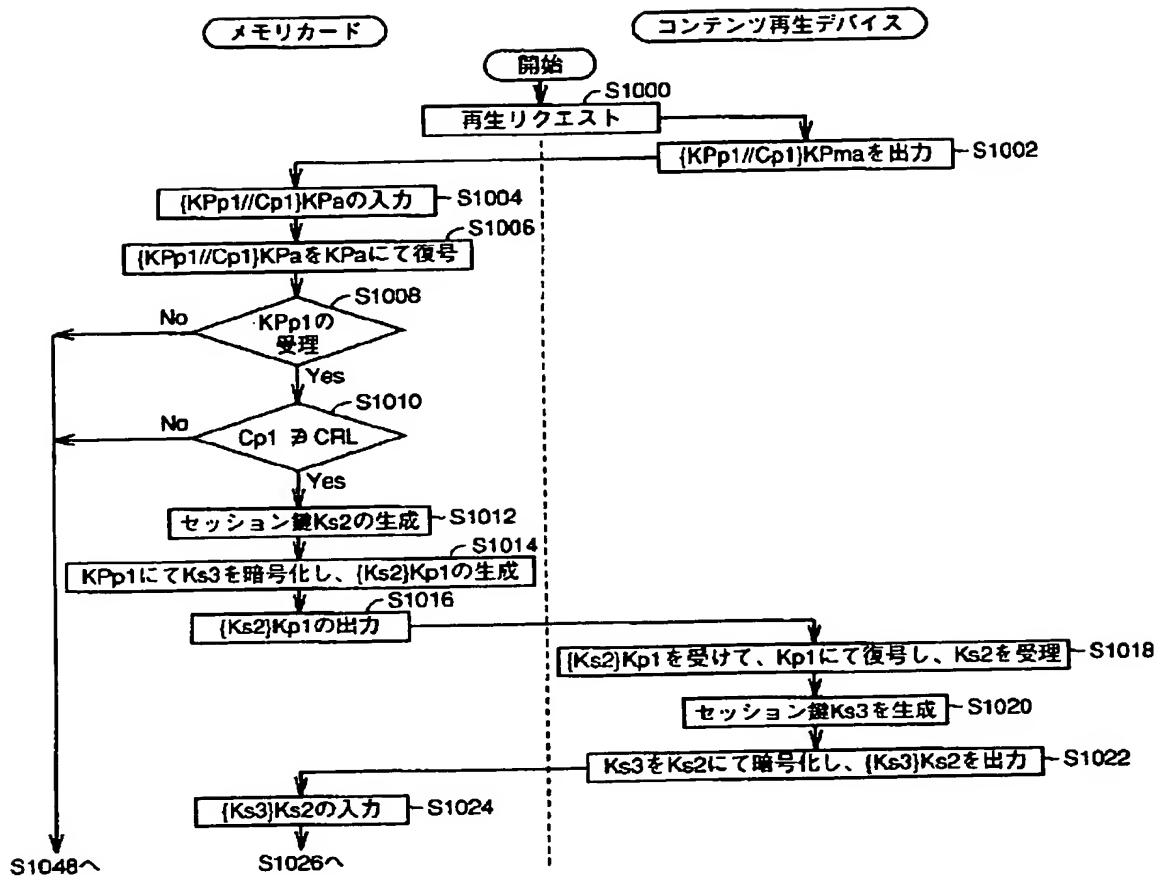
【図18】



【図22】



【図20】



フロントページの続き

(51) Int. Cl. 7

識別記号

G 1 0 K 15/02
G 1 0 L 11/00
H 0 4 L 9/08

F I

H 0 4 L 9/00
G 1 0 L 9/00
H 0 4 L 9/00

テーマコード(参考)

6 7 5 B
E
6 0 1 C
6 0 1 E

(71) 出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(71) 出願人 000004167
日本コロムビア株式会社
東京都港区赤坂4丁目14番14号
(72) 発明者 堀 吉宏
大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内
(72) 発明者 上村 透
大阪府守口市京阪本通2丁目5番5号 三
洋電機株式会社内

(72) 発明者 畠山 卓久
神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内
(72) 発明者 高橋 政孝
石川県河北郡宇ノ気町宇野気ヌ98番地の
2 株式会社ピーエフユー内
(72) 発明者 常広 隆司
神奈川県横浜市戸塚区吉田町292番地 株
式会社日立製作所システム開発研究所横浜
ラボラトリ内

(72)発明者 大森 良夫

神奈川県川崎市川崎区港町5番1号 日本
コロムビア株式会社川崎工場内

Fターム(参考) 5J104 AA07 AA13 AA15 AA16 EA06
EA19 KA02 KA05 NA02 NA03
NA06 NA35 NA37 NA38 NA41
NA42 PA07 PA11